CLAUDIO DELAINI

INTELLIGENZA ARTIFICIALE: I RISCHI NELLE FABBRICHE

GUIDA PER CHI VUOLE IMPLEMENTARE L'IA NEGLI STABILIMENTI INDUSTRIALI

con il contributo
Massimo Marini,
Roberto Serra e
dell'avv. Silvia Zuanon

Claudio Delaini

INTELLIGENZA ARTIFICIALE: I RISCHI NELLE FABBRICHE

Guida per chi vuole implementare l'AI negli stabilimenti industriali

certificazionece.it

Copyright Claudio Delaini
1^ edizione aprile 2025
Titolo: INTELLIGENZA ARTIFICIALE: I RISCHI NELLE FABBRICHE
Guida per chi vuole implementare l'AI negli stabilimenti industriali
Autore: Claudio Delaini
Tutti i diritti riservati: Nessuna parte di questa pubblicazione può essere memorizzata, fotocopiata o riprodotta senza le dovute autorizzazioni. Chiunque favorisca questa pratica commette un illecito perseguibile a norma di legge.

Codice ISBN: 979-12-210-2985-7
Casa editrice: Independently published

Fotografa il QR per avere tutti i miei riferimenti

Sommario

Introduzione 7

1 Intelligenza artificiale e macchinari industriali: una definizione complicata 13

2 La normativa sull'intelligenza artificiale in fabbrica: AI ACT e Regolamento Macchine 17

- Cos'è l'AI Act, quando è entrato in vigore e quando diventa obbligatorio 17
- Classificazioni di rischio nell'AI Act e macchinari industriali 18
- Regolamento Macchine e macchinari che usano l'intelligenza artificiale 22
- Tiriamo le somme 25

APPROFONDIMENTO: **RIVOLUZIONE IA: LE VERE OPPORTUNITÀ E I RISCHI PER LE AZIENDE** 26

3 I rischi per la sicurezza legati all'intelligenza artificiale 31

- Errori software e allucinazioni dell'IA 31
- Rischi legati alla sicurezza informatica 32
- Rischio di perdita di controllo umano 33
- Rischi di isolamento e tecnostress 34

4 Responsabilità giuridiche e intelligenza artificiale: chi risponde degli errori? 37

- Normativa sull'intelligenza artificiale: uno scenario ancora in evoluzione 37
- Responsabilità in caso di errore 38

- Responsabilità in caso di danni a terzi 42
- Responsabilità dell'AI e contratti: attenzione alle clausole 44
- Per riassumere 45

5 Intelligenza artificiale e trattamento dei dati sensibili (GDPR) 47
- Intelligenze artificiali e protezione dei dati sensibili: legittimità del trattamento 48
- Trasferimento dei dati sensibili verso server di terze parti e verso altri Paesi 49
- In sintesi: a cosa fare attenzione 50

6 Un caso specifico: i chatbot per l'assistenza tecnica che usano l'IA 51
- Premessa: i vantaggi dei chatbot di assistenza che usano l'IA 51
- I rischi specifici 53
- Tiriamo le somme 55

APPROFONDIMENTO: **L'AI ACT, SPIEGATO SEMPLICE 57**

APPROFONDIMENTO: **IN ITALIA, L'INTELLIGENZA ARTIFICIALE NEL MONDO DEL LAVORO È ANCORA SOTTOVALUTATA 101**

APPROFONDIMENTO: **CASE STUDY: USARE L'INTELLIGENZA ARTIFICIALE PER SEMPLIFICARE I PROCESSI DI GESTIONE DELLE INFORMAZIONI IN AZIENDA 111**

Note sull'autore e Contributors 116

INTELLIGENZA ARTIFICIALE: I RISCHI NELLE FABBRICHE

Guida per chi vuole implementare l'AI negli stabilimenti industriali

Introduzione

Ti ricordi di quando, qualche anno fa, si è iniziato a parlare di intelligenza artificiale?

Io sì. Forse, un giorno, potrò dire ai miei nipoti: *io c'ero*.

Allora, però, l'intelligenza artificiale sembrava qualcosa di distante, che riguardava un remoto futuro. Le intelligenze artificiali erano sinonimo di film di fantascienza: evocavano i personaggi di Blade Runner, il protagonista di Terminator o il malvagio agente Smith di Matrix. Insomma, qualcosa di lontanissimo dai macchinari industriali e dal mondo delle fabbriche che frequento ogni giorno.

Ma se la tecnologia ci ha insegnato qualcosa negli ultimi decenni, è che il futuro è già qui. Nel frattempo, infatti, le intelligenze artificiali hanno perso i tratti sinistri dei personaggi di fantasia, per assumere il volto servizievole – e talora un po' stupido – di Chat GPT e affini.

Eh sì, se fino a poco tempo fa l'intelligenza artificiale sembrava ancora lontana dall'avere concrete ricadute nella vita di ogni giorno, negli ultimi anni (e, ancor più, negli ultimi mesi) abbiamo assistito in diretta ad un'incredibile accelerazione.

Oggi, nel 2025, anche nelle fabbriche vediamo con sempre maggiore frequenza delle applicazioni delle IA, che vengono usate per rendere più efficienti e rapide alcune operazioni.

Qualche esempio concreto? Eccone un po':

- **I chatbot IA per l'assistenza tecnica dei macchinari**, che aiutano gli operatori a risolvere problemi fornendo risposte rapide basate su manuali e documenti tecnici, grazie a software in grado di estrarre e rielaborare informazioni complesse.
- **I magazzini automatizzati**, sistemi intelligenti che organizzano lo stoccaggio e la movimentazione delle merci, riducendo tempi ed errori.
- **I veicoli a guida autonoma**, piccoli robot che trasportano materiali all'interno degli stabilimenti senza intervento umano.
- **I sensori per la manutenzione predittiva**, che rilevano in tempo reale anomalie nei macchinari, prevenendo guasti improvvisi e migliorando la pianificazione della manutenzione.
- **I sistemi di analisi predittiva degli incident**i, algoritmi che analizzano dati storici e attuali per identificare potenziali situazioni di rischio prima che si verifichino.
- **I dispositivi di monitoraggio dei parametri vitali degli operatori**, che controllano battito cardiaco, temperatura e altri parametri per prevenire incidenti o malori sul lavoro.
- **I sensori di controllo dei DPI con tecnologia RFID**, che garantiscono che i lavoratori indossino correttamente i dispositivi di protezione individuale, segnalando eventuali mancanze.

Nota importante: questi che ho citato ora sono generalmente classificati come sistemi che utilizzano l'intelligenza artificiale, ma su questa definizione si potrebbe discutere. Capiremo perché nel primo capitolo del libro

Sai che c'è, però? C'è che viviamo nel bel mezzo di un paradosso.

Da un lato, infatti, assistiamo ad una proliferazione dell'intelligenza artificiale in fabbrica, che occupa sempre più spazio nell'organizzazione, la logistica e la produzione – ma anche in settori che

interessano più direttamente la sicurezza sul lavoro: manutenzione, prevenzione, controllo.

Dall'altro lato, abbiamo sistemi normativi che provano a rincorrere le novità velocissime del mondo delle intelligenze artificiali, cercando di regolarle e irreggimentarle in qualche modo. Va letto in questo senso il recente **AI Act** promulgato dall'Unione Europea, uno dei primi strumenti legislativi al mondo che si propone di sottoporre a normative e controlli sistematici le intelligenze artificiali e il loro processo produttivo.

Nonostante gli aspetti positivi dell'AI Act, bisogna essere consapevoli che si tratta solo di un primo passo, per molti versi ancora carente. Il Regolamento europeo sull'intelligenza artificiale prende infatti in considerazione soprattutto gli aspetti di pericolo macroscopici dell'intelligenza artificiale – come la possibile violazione dei diritti umani e la guida occulta dell'opinione pubblica – rispetto ai rischi concreti a cui ci pone di fronte il suo utilizzo nelle fabbriche.

In questo scenario complesso, come si valuta e si gestisce la sicurezza dei macchinari che sfruttano l'intelligenza artificiale? A quale quadro normativo si fa riferimento? Quali responsabilità ci si assume inserendo negli stabilimenti dei sistemi che usano l'IA?

Questo libro nasce proprio per rispondere a queste domande. Si tratta di un approfondimento necessariamente temporaneo e provvisorio, proprio perché la materia di cui trattiamo è calda, viva, in continuo fermento e costante evoluzione.

L'obiettivo è fare il punto sullo stato dell'arte dell'intelligenza artificiale nelle fabbriche oggi (aprile 2025). Il mio proposito, poi, è quello di tenere aggiornata questa pubblicazione. In ogni caso continuerò a trattare questo tema sul blog e sui miei canali social, quindi puoi informarti sulle novità anche da lì.

Di cosa parleremo in questo libro?

Per prima cosa cercheremo di capire cos'è effettivamente e come si può definire l'intelligenza artificiale così come viene usata nelle fabbriche. Si tratta di una domanda solo apparentemente scontata, che invece stimola riflessioni e considerazioni interessanti.

In seguito analizzeremo le principali normative che attualmente regolano l'uso dell'AI in fabbrica, ovvero AI Act e Regolamento Macchine.

Il terzo capitolo sarà invece dedicato alla valutazione e prevenzione dei rischi legati all'IA. Successivamente, nei capitoli quattro e cinque, ci apriremo a questioni più squisitamente giuridiche: analizzeremo le responsabilità giuridiche legate all'IA e la questione del trattamento dei dati sensibili. Infine proveremo a mettere le mani in pasta, prendendo in considerazione un esempio pratico di intelligenza artificiale in uso nelle fabbriche: i chatbot di assistenza tecnica.

Il libro è corredato dai preziosi interventi di tre professionisti (e amici) che ci aiuteranno ad avere una panoramica più completa sul mondo dell'intelligenza artificiale:

- **Roberto Serra** (esperto di marketing digitale e Search Engine Optimization) ci porterà a capire le sfide e le opportunità che le Intelligenze artificiali presentano per le aziende produttive, e come si stanno recependo queste tecnologie in Italia e nel resto del mondo;
- **Silvia Zuanon** (avvocato d'impresa) ci aiuterà a "decifrare" l'AI Act e ci supporterà nel cercare di comprendere le responsabilità giuridiche e le necessità sul trattamento dei dati sensibili collegati all'uso delle intelligenze artificiali;
- **Massimo Marini** (direttore commerciale di Analysis,un'azienda che da 30 anni sviluppa software per rendere più efficienti i processi

aziendali) ci illustrerà un caso reale di utilizzo dell'intelligenza artificiale collegato ad un software di gestione documentale, svelando i vantaggi, le potenziali difficoltà e i passaggi di implementazione tecnologica.

Spero che, nell'insieme, questo approfondimento possa aiutare imprenditori, RSPP e responsabili della sicurezza ad avere un quadro più chiaro, e a capire meglio come muoversi all'interno di un contesto ancora fumoso.

E ora preparati ad affinare la mente e a fare qualcosa che l'intelligenza artificiale non sa ancora replicare (forse): entrare nella complessità, nei "se" e nei "ma", e, dal caos, estrarre una parvenza d'ordine.

1 Intelligenza artificiale e macchinari industriali: una definizione complicata

Nell'ultimo anno mi è capitato spesso, visitando fabbriche, che i miei clienti mi dicessero tutti esaltati: "Guarda, stiamo creando questo prodotto/attivando questo macchinario che usa l'intelligenza artificiale".

Onestamente, io mi sono spesso sentito un po' a disagio. Eh sì, perché nell'ambito dei macchinari industriali non è così facile capire quando possiamo davvero parlare di intelligenza artificiale!

Proviamo allora a leggere la definizione di intelligenza artificiale che è stata inserita nell'AI Act:

«Sistema di IA»: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
[Articolo 3 del Regolamento UE 2024/1689]

Gli elementi chiave per definire un sistema di IA sarebbero, quindi:

- Una certa autonomia (si parla di livelli variabili);
- L'adattabilità dopo la diffusione (la famosa autoevoluzione);
- La generazione di output – previsioni, contenuti, raccomandazioni o decisioni – che influenzano l'ambiente circostante, sia esso reale o digitale.

A fronte di tutti i discorsi che si fanno oggi sull'IA, bisogna considerare che **questa è, per ora, l'unica definizione di intelligenza artificiale inserita in un quadro normativo.**

Il problema è che questa definizione è molto generica. Tanto per dirne una, qualsiasi macchina genera degli output sulla base di input, ad esempio sulla base di vincoli e lavorazioni che abbiamo determinato in precedenza.

Insomma, con questa definizione si possono considerare sistemi di intelligenza artificiale anche dispositivi che esistevano ben prima che si parlasse di AI nelle fabbriche!

Qualche esempio? I magazzini automatizzati che decidono quali articoli prendere e con quale percorso, dove l'operatore ha soltanto un ruolo di supervisione. Oppure le linee di imbottigliamento che in base ad una serie di dati (il tasso di umidità dell'aria, la temperatura ecc) decidono come gestire la colorazione.

Ma possiamo veramente parlare di intelligenza artificiale per questi tipi di macchinari?

Dopo aver approfondito l'argomento, ascoltando vari specialisti del settore, io mi sono fatto un'opinione, che è però personalissima e da "inesperto" – dopotutto sono un consulente sulla sicurezza dei macchinari, non un ingegnere informatico.

La mia risposta è: sì e no.

Nei casi che ho citato, così come nella definizione dell'Unione Europea, non si trova traccia di un elemento essenziale delle intelligenze artificiali: **l'elaborazione di grandi quantità di dati su base statistica per prendere decisioni.**

In questo senso, quasi tutte le forme di intelligenza artificiale che sono presenti oggi nelle fabbriche sono da considerarsi necessariamente imperfette e immature, per il semplice motivo che non hanno abbastanza dati a disposizione per prendere decisioni sensate.

Tra cinque anni, probabilmente, questo problema non ci sarà più. Ad oggi, nel 2025, bisogna ancora tenerne conto. Questo è il motivo per cui, nell'ambito fabbrica, possiamo parlare di intelligenze artificiali solo limitatamente.

La metto giù in un altro modo. La maggior parte delle intelligenze artificiali che si trovano oggi nelle fabbriche sono come bambini di cinque o sei anni. Sono proprio simili a piccoli essere umani: riescono sì ad esprimersi, a fare delle affermazioni, ma quello che dicono è spesso impreciso o esagerato. Hanno quindi bisogno della tutela e del supporto di "un adulto" che interpreti quello che stanno dicendo e che distingua tra verità ed esagerazione.

[Sono il fiero papà di due gemelle di quell'età, quindi so bene di cosa parlo].

Fuor di metafora, i risultati prodotti oggi dall'intelligenza artificiale devono essere vagliati e convalidati da un esperto umano. Magari tra cinque anni non sarà più così, questo non lo so dire.

Oggi come oggi, però, quasi tutte le IA usate nelle fabbriche non hanno a disposizione abbastanza dati (e feedback) perché le soluzioni che propongono vengano adottate senza un passaggio di validazione umana.

Questo è un concetto fondamentale che vorrei passare, perché ha ricadute gigantesche sulla sicurezza, la valutazione dei rischi e la gestione delle responsabilità. Insomma, se dovessi dimenticare tutto quel che leggerai in questo libro, ti prego di ricordare almeno questo!

2 La normativa sull'intelligenza artificiale in fabbrica: AI ACT e Regolamento Macchine

Cos'è l'AI Act, quando è entrato in vigore e quando diventa obbligatorio

Il 1° agosto 2024 è entrato in vigore l'AI Act, ovvero il Regolamento europeo sull'Intelligenza Artificiale. Tuttavia, come per tutte le normative europee, è previsto un periodo di transizione in cui il regolamento è in vigore ma non è ancora obbligatorio adottarlo. La data di piena applicazione dell' AI Act è infatti il 2 agosto 2026, due anni dopo la prima entrata in vigore.

Con l'AI Act, l'Unione Europea ha provato in qualche modo a regolamentare il campo completamente nuovo dell'intelligenza artificiale. Le finalità dei legislatori sarebbero quelle di garantire:

- La sicurezza, facendo sì che i prodotti che utilizzano l'intelligenza artificiale non danneggino le persone;
- La trasparenza, assicurando che gli utilizzatori possano capire come funziona l'AI e su quali basi vengono prese le decisioni.

Il condizionale che ho usato fin qui è d'obbligo, perché l'AI Act rappresenta appunto un tentativo dell'Unione Europea di avventurarsi in un campo non solo recentissimo, ma anche in costante espansione ed evoluzione.

Per provare a mappare e normare questo territorio sconosciuto, i legislatori europei hanno tirato fuori dal cassetto uno strumento che conosciamo molto bene: **la certificazione CE.**

In altre parole, i prodotti che utilizzano l'intelligenza artificiale e che vengono prodotti o venduti nell'Unione Europea dovranno (o dovrebbero) rispettare gli standard di sicurezza europei – compresi quelli sulla valutazione del tipo di rischio – per ottenere la certificazione CE che li rende commerciabili in Europa.

Forse qualcuno ricorderà che già nel Regolamento Macchine si iniziava a parlare di intelligenza artificiale, ma tutti aspettavamo la versione definitiva del regolamento sull'intelligenza artificiale per capire meglio come gestire gli aspetti relativi alla sicurezza.

E quindi ora che è stato approvato l'AI Act è tutto a posto, giusto?

Non proprio. Come cercherò di spiegarti nei prossimi paragrafi, non è ancora del tutto chiaro come applicare la nuova norma, almeno per quanto riguarda i macchinari industriali che sfruttano l'intelligenza artificiale.

Classificazioni di rischio nell'AI Act e macchinari industriali

Come ho accennato prima, nel Regolamento Macchine si parla di macchine che utilizzano l'intelligenza artificiale, ma senza specificare come si devono valutare i rischi di questi macchinari.

Nel Regolamento europeo sull'intelligenza artificiale (AI Act) si stabiliscono invece 4 diversi livelli di rischio:

1) Rischio inaccettabile

Comprende i sistemi che violano i diritti umani e i valori fondamentali dell'Unione Europea, quali ad esempio la sorveglianza di massa. I sistemi AI di questo tipo sono vietati all'interno dell'Unione Europea.

2) Alto rischio

Comprende sistemi che potrebbero causare danni significativi in caso di malfunzionamento: sistemi di identificazione biometrica e riconoscimento facciale, sistemi di valutazione del credito e scoring, chatbot medici, sistemi di guida autonoma...

3) Rischio limitato

Comprende sistemi che presentano un rischio minore, come chatbot generici o software di elaborazione delle immagini. Il rischio è associato, in questo caso, alla potenziale mancanza di trasparenza. Parlando dei chatbot, ad esempio, gli utenti devono essere informati che non stanno interagendo con un essere umano, così come deve essere chiaro che le immagini elaborate dai software non sono fotografie reali.

4) Rischio minimo

Si tratta di sistemi con un impatto minimo o nullo sui diritti o la sicurezza delle persone. La loro funzione principale è aiutare a organizzare le attività quotidiane senza incidere su decisioni o attività di rilevanza critica. Un'app di gioco con l'IA per il cellulare potrebbe ad esempio rientrare in questa categoria.

Tutto questo è spiegato in modo molto più approfondito nell'intervento dell'avvocato Silvia Zuanon a pagina 57, che ci guida passo per passo nell'analisi del Regolamento europeo sull'intelligenza artificiale

Proviamo ad analizzare meglio queste categorie per capire dove potremmo inserire i nostri macchinari industriali.

Nella prima categoria, **rischio inaccettabile**, sicuramente non rientrano le macchine. Qui si parla di intelligenze artificiali in grado di influenzare le masse, di utilizzo dei dati biometrici e altre tematiche importantissime, ma che nulla hanno a che fare con le fabbriche.

Insomma, per i macchinari non dovrebbe esistere rischio inaccettabile.

Passiamo alle **tecnologie ad alto rischio**, ovvero i sistemi che possono causare danni significativi in caso di malfunzionamento. In questi casi entrano in gioco questioni di sicurezza e affidabilità del software, che in parte vengono già applicate in campo medicale, dove è necessario essere certi delle diagnosi e dei risultati. Pensa all'importanza di avere risultati certi quando, ad esempio, si fa un'ecografia morfologica in cui si scoprono le malformazioni del feto.

I sistemi di intelligenza artificiale considerati ad alto rischio saranno sottoposti ad una serie di misure di sicurezza più rigorose: dovranno essere certificati da enti esterni, verranno inseriti in un registro pubblico e dovranno essere sottoposti a controlli periodici in seguito all'immissione sul mercato. Inoltre, le richieste relative a sicurezza e affidabilità dei dati, tracciabilità dei risultati e documentazione sono, chiaramente, più severe.

E i nostri macchinari industriali?

Se ci limitiamo alla definizione generale, i macchinari potrebbero rientrare in questa categoria: una macchina o un componente di sicurezza può causare un infortunio o addirittura una morte accidentale, quindi potrebbe essere considerata ad alto rischio

Tuttavia nelle varie tipologie di esempi inserite nell'allegato III dell'AI Act (quello che tratta i sistemi ad alto rischio) non si parla mai di macchinari industriali.

Sistemi a rischio limitato. In questa categoria rientrano le IA che già tutti conosciamo e utilizziamo: chat GPT che ci risponde alle domande, l'IA di Linkedin che elabora un'immagine sulla base del titolo di un messaggio eccetera. Anche qui, tuttavia, l'AI Act non fa riferimenti specifici a macchinari, e lo stesso vale per **i sistemi a**

rischio minimo.

Inizi a capire anche tu qual è il problema dell'AI Act?

Diciamolo chiaro e tondo: **in questo nuovo regolamento europeo i macchinari non compaiono affatto**. Non solo, non si parla nemmeno di oggetti che utilizzano la tecnologia!

Come classifichiamo la lavatrice che usa l'AI per suggerirti la migliore modalità di lavaggio? E il robottino aspirapolvere che individua in modo intelligente gli ostacoli e capisce se sta passando su un tappeto o sul parquet?

Queste sono tutte applicazioni dell'intelligenza artificiale che sono già tra di noi, che si trovano in qualsiasi negozio di elettrodomestici. Ma nell'AI Act tutta l'attenzione si è concentrata sui sistemi di intelligenza artificiale più complessi (e anche più pericolosi) tralasciando le applicazioni più immediate. Certo, verrebbe da dire che con questi oggetti il rischio sarà limitato o minimo, ma qui entriamo nella libera interpretazione della norma...

Lo stesso identico discorso vale per i macchinari. Nell'AI Act non sono presi in considerazione, ad esempio, i software di assistenza dei macchinari, che già esistono e si usano. **Inoltre, al momento mancano completamente le norme tecniche necessarie per produrre e per classificare il rischio dei macchinari o delle componenti che usano l'IA nelle fabbriche.**

Regolamento Macchine e macchinari che usano l'intelligenza artificiale

Visto che nell'AI Act non si trovano accenni specifici su come trattare i macchinari o le componenti che usano l'intelligenza artificiale, dobbiamo necessariamente andare a vedere i regolamenti di prodotto. Nel caso dei macchinari, il riferimento fondamentale è il nuovo Regolamento Macchine 2023/1230.

Effettivamente il Regolamento Macchine (approvato prima dell'AI Act) si occupa di intelligenza artificiale, anche se la chiama sistema o comportamento autoevolutivo. Nel Regolamento Macchine, in particolare, vengono citati:

- *Macchine che integrano sistemi con un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza che non sono state immesse in modo indipendente sul mercato, solo per quanto riguarda tali sistemi.*
- *Componenti di sicurezza dotati di un comportamento integralmente o parzialmente autoevolutivo che utilizzano approcci di apprendimento automatico che garantiscono funzioni di sicurezza.*

Queste definizioni sono tratte **dall'allegato I del Regolamento Macchine**, ovvero l'allegato che dettaglia macchinari e componenti considerati ad alto rischio e che devono necessariamente essere certificati CE da un ente notificato.

Detto in un altro modo, un'interpretazione stringente del Regolamento Macchine obbligherebbe tutti i macchinari e componenti che usano l'IA a ricevere la certificazione CE solo tramite ente notificato.

Il problema, però, è che al momento non esistono norme UNI, CEI, ISO che spieghino come certificare un software di intelligenza

artificiale. E i RES indicati nel Regolamento Macchine sono troppo generici rispetto a questo ambito, quindi non risultano funzionali a questo tipo di valutazione.

E quindi come devono fare i consulenti di sicurezza come me, chi lavora negli enti notificati o gli impiegati ministeriali che devono controllare le certificazioni dei macchinari o dei componenti che utilizzano l'AI?

Di fatto, in questo momento non abbiamo gli strumenti per muoverci in questo senso.

Come si procede, allora? Eh, bisogna per forza di cose classificare i software di intelligenza artificiale non tanto come "componenti di sicurezza" ma come aventi "funzione di sicurezza". Vediamo la differenza delle due definizioni nel Regolamento Macchine:

- *«componente di sicurezza»: un componente fisico o digitale, compreso un software, di un prodotto rientrante nell'ambito di applicazione del presente regolamento, che è progettato o destinato ad espletare una funzione di sicurezza e che è immesso sul mercato separatamente, il cui guasto o malfunzionamento mette a repentaglio la sicurezza delle persone, ma che non è indispensabile per il funzionamento di tale prodotto, o per il quale componenti normali possono essere sostituiti per il funzionamento di tale prodotto;*
- *«funzione di sicurezza»: una funzione che serve a soddisfare una misura di protezione destinata a eliminare o, se ciò non è possibile, a ridurre un rischio, e che, se ha un guasto potrebbe comportare un aumento di tale rischio;*

Cosa significa questo, in soldoni? Semplice: gli elementi che espletano una funzione di sicurezza non devono passare al vaglio di un ente notificato. La certificazione CE resta, come nella maggior parte dei casi, un'autocertificazione.

Il software IA che muove il robot automatizzato, l'intelligenza artificiale che serve per fare la manutenzione preventiva e predittiva alle valvole dell'oil e gas, il software documentale con AI che integra i manuali cartacei sono tutti esempi di software che non vengono venduti separatamente, ma che sono integrati al macchinario o al componente. Di conseguenza possono essere esclusi dalla definizione di componenti di sicurezza ed essere considerati elementi che espletano funzioni di sicurezza. Tutto chiaro fin qua?

Attenzione, però. Questa soluzione che sto indicando non è una scappatoia per rendere più semplice il processo di certificazione. *Semplicemente, sto constatando che allo stato attuale della normativa questa è l'unica soluzione possibile per arrivare a immettere sul mercato macchinari e componenti che utilizzano l'intelligenza artificiale.*

Quando arriveranno le norme tecniche, che sicuramente arriveranno, saremo tutti più sereni. I produttori avranno degli standard a cui attenersi, e chi si occupa di sicurezza avrà dei riferimenti precisi. Per ora, però, la situazione è questa.

Consideriamo anche che, per quanto abbiamo visto in precedenza, la maggior parte degli utilizzi dell'intelligenza artificiale in fabbrica andranno probabilmente a rientrare nella classificazione di rischio minimo dell'AI Act (classificazione che non richiede l'intervento di un ente certificato).

Nel Regolamento Macchine, al contrario, ogni macchinario o componente di sicurezza con comportamento autoevolutivo viene automaticamente considerato ad alto tasso di pericolo e richiederebbe il passaggio dell'ente certificato.

Sappiamo, però, che il Regolamento Macchine è uscito prima dell'AI Act. Quindi, a logica, è l'AI Act che dovrebbe fare da riferimento. Ma,

come detto, l'AI Act non si occupa nello specifico di macchinari...

Insomma, c'è una contraddizione tra i due regolamenti che al momento non si sa bene come gestire o risolvere, se non utilizzando la strada della "funzione di sicurezza" che ti ho indicato prima.

Tirando le somme

In questo capitolo ci siamo detti tante cose. Proviamo a riassumerle:

- L'AI Act non contiene specifici riferimenti su come valutare il rischio di macchinari e componenti di macchinari che utilizzano l'intelligenza artificiale. È quindi necessario risalire alla normativa di prodotto, in questo caso il Regolamento Macchine 2023;
- Il Regolamento Macchine inserisce macchinari e componenti che usano l'IA nell'elenco di macchine che richiedono l'intervento di un ente terzo per ricevere la certificazione CE;
- Al momento non esistono norme tecniche a cui fare riferimento per la sicurezza dei software di AI utilizzati nelle fabbriche. Questo rende di fatto impossibile far certificare tali software da un ente esterno;
- Se i software che usano l'IA sono integrati al macchinario o al componente, è possibile considerarli come elementi che hanno una "funzione sicurezza" anziché "componenti di sicurezza". In questo caso si può seguire la strada dell'autocertificazione per la conformità CE.

Ti invito ad andare alla pagina 57 e leggere l'illuminante sintesi dell'AI Act redatta dall'avvocato Silvia Zuanon.

APPROFONDIMENTO A CURA DI

Roberto Serra

Esperto di marketing digitale
e Search Engine Optimization

RIVOLUZIONE IA: LE VERE OPPORTUNITÀ E I RISCHI PER LE AZIENDE

Spesso sento dire che l'intelligenza artificiale è un po' come la rivoluzione industriale, nel senso che ha la potenzialità di cambiare tutto il nostro modo di lavorare. E, in effetti, sotto molti punti di vista è proprio così. C'è però una distinzione fondamentale tra rivoluzione industriale e rivoluzione dell'IA. Eh sì, perché questa volta non stiamo sostituendo l'uomo solo nella parte meccanica del lavoro – quella più "attuativa", per intenderci. Stiamo andando a toccare la parte "pensante", quella decisionale.

Se la rivoluzione industriale ha rimpiazzato la carrozza a cavalli con il treno, quello che stiamo facendo ora è sostituire l'omino che decide se usare la carrozza o il treno. Una bella differenza, non trovi?

Detto questo, ci sono almeno due punti su cui bisogna assolutamente fare chiarezza quando si parla di intelligenza artificiale. Il primo riguarda cos'è l'IA, mentre il secondo è relativo al come usare l'IA nelle aziende.

Partiamo dal primo. Troppo spesso si identifica l'intelligenza artificiale con i Large Language Model di carattere generativo come Chat GPT e simili. Parlo di quei modelli a cui si pongono domande e che forniscono risposte sotto forma di output di testo. In realtà il mondo dell'intelligenza artificiale è molto più vasto e complesso, e offre molte più possibilità. La vera opportunità per le aziende, soprattutto per le aziende di tipo produttivo, sta nella capacità delle IA di ragionare a partire dai dati.

Ecco che, allora, la gestione dei dati aziendali diventa il punto cruciale. Le informazioni amministrative o logistiche degli ultimi vent'anni, che hai conservato quasi solo per scrupolo, possono diventare un vero tesoro, la base di partenza da cui le IA possono fare ragionamenti di tipo predittivo.

Facciamo un esempio. Hai un'azienda che produce cacciaviti. L'intelligenza artificiale potrebbe aiutarti a prevedere con una certa precisione gli ordini che arriveranno nel prossimo futuro, e potrebbe di conseguenza suggerirti come gestire in modo più efficiente il magazzino. Potrebbe inoltre aiutarti a capire quali tipologie di cacciaviti sono più richieste, quali danno più problemi e come ottimizzare la produzione. Potrebbe addirittura supportarti nel far evolvere la tua offerta o il tuo prodotto. Ma per fare tutto questo l'intelligenza artificiale ha bisogno di dati, dati che devono essere proprietari (cioè tuoi) e puliti, ovvero catalogati e conformi per essere dati in pasto all'IA.

Qui però si apre un altro tema scottante: quello della privacy. Dare in pasto i dati a grandi società come quelle che gestiscono GPT significa in qualche modo perderne il controllo. Le intelligenze artificiali sono infatti molto diverse dai software database o dagli archivi che abbiamo utilizzato fino ad oggi. Per capirsi, i

database vecchio stampo sono simili a dei mobiletti con i cassetti: se si svuota il cassetto (cioè, se si elimina il dato), il contenuto scompare. Al contrario, le intelligenze artificiali funzionano in una dimensione vettoriale, in cui è praticamente impossibile cancellare un dato inserito. Detto in un altro modo, quando le IA "imparano" qualcosa, il processo non è invertibile. Capisci bene, dunque, che problemi emergono quando sottoponi all'intelligenza artificiale un brevetto aziendale...

Questa è la vera sfida dei prossimi anni e l'aspetto su cui probabilmente si concentreranno la maggior parte degli sforzi sull'intelligenza artificiale in ambito aziendale. Bisognerà capire come far funzionare le IA localmente, all'interno della propria azienda o organizzazione, senza che quei dati sensibili escano all'esterno. E poi si dovrà comprendere come sottoporre dati puliti e utilizzabili alle IA per ottenere ragionamenti predittivi che ci aiutino a prendere decisioni.

Insomma, per gli imprenditori l'opportunità vera dell'intelligenza artificiale non sta tanto nelle risposte che può fornire Chat GPT, ma nel capire come integrare nella propria organizzazione uno degli strumenti più potenti della storia dell'essere umano e usarlo per migliorare la produzione, rendere più efficiente l'azienda e predire andamenti e tendenze future.

Ovviamente a questa grande opportunità si accompagnano dei rischi. Quello della privacy, di cui abbiamo parlato, è un tema da tenere in seria considerazione. Ma oggi, in un momento in cui siamo agli albori dell'IA, c'è anche il pericolo di lasciarsi sfuggire il momento e restare indietro rispetto ai concorrenti, o, al contrario, di sprecare energie e risorse facendosi inghiottire dal vortice di questo universo dalle mille sfaccettature.

Il mio consiglio per gli imprenditori che si approcciano a questo mondo è di provare a sfruttare l'intelligenza artificiale in modo che abbia ricadute pratiche sul mondo reale. Meglio concentrarsi su un singolo processo alla volta, identificando l'area in cui l'IA può portare un beneficio concreto, e lavorare su quell'obiettivo fino ad ottenere risultati veri e misurabili.

3 I rischi per la sicurezza legati all'intelligenza artificiale

Nel capitolo precedente abbiamo parlato di come AI Act e Regolamento Macchine indichino strade apparentemente diverse per normare macchinari e software che fanno uso dell'intelligenza artificiale. In entrambi i casi, però, abbiamo una certezza: **i prodotti che usano le IA devono essere certificati CE.**

Ora, come tutti sappiamo, **la valutazione dei rischi** è una componente fondamentale della marcatura CE. Ma per questa valutazione bisognerà tener conto di alcuni rischi specifici, propri delle intelligenze artificiali.

In questo capitolo proviamo ad individuare proprio quali rischi "caratteristici" potrebbero essere associati alle intelligenze artificiali. L'elenco che segue non sarà sicuramente esaustivo, né punta ad esserlo. Come già detto, dobbiamo aspettare la pubblicazione le linee guida tecniche dell'AI Act per avere delle indicazioni più chiare sulla valutazione dei rischi. Nel frattempo, però, da qualche parte bisogna pur partire!

Ti suggerisco quindi di usare questo elenco come un canovaccio, una mappa generale che indica la strada, ma che va poi calata nel tuo caso specifico, prestando attenzione alle peculiarità del tuo macchinario o software a base di intelligenza artificiale.

Errori software e allucinazioni dell'IA

Uno dei rischi principali legati all'uso dell'intelligenza artificiale nelle

fabbriche è rappresentato dagli **errori del software** , che possono portare a guasti e malfunzionamenti, e dalle cosiddette **"allucinazioni" dell'IA**, ovvero risposte o analisi sbagliate generate dai sistemi di intelligenza artificiale.

Ad esempio, un'IA utilizzata per la manutenzione predittiva dei macchinari potrebbe segnalare un guasto inesistente o, al contrario, non rilevare un problema reale, con conseguenze potenzialmente gravi sulla produttività o sulla sicurezza.

Come contrastare il rischio?

Per mitigare questo rischio è fondamentale introdurre **un passaggio di validazione umana obbligatorio**: le decisioni prese dall'IA devono essere confermate da un operatore esperto prima di essere attuate

Nel caso dell'IA usata per la manutenzione, ad esempio, ci sarà bisogno del "via libera" di un manutentore. Se si utilizza l'intelligenza artificiale per tradurre il manuale d'uso di un macchinario in una lingua straniera, il risultato dovrà essere passato al vaglio di un traduttore professionista, e così via.

Inoltre, per tutelarsi da eventuali danni causati da errori del sistema, può essere utile stipulare un'assicurazione che copra le perdite economiche o i danni materiali legati a malfunzionamenti o interpretazioni errate dell'IA. Questo vale soprattutto in settori ad alto rischio: pensa ad esempio all'entità dei danni che può causare un sensore IA che commette un errore nei settori oil and gas...

Rischi legati alla sicurezza informatica

Tra i rischi più importanti nell'uso dell'intelligenza artificiale in fabbrica c'è quello legato alla sicurezza informatica. Sistemi come veicoli autonomi, sensori intelligenti o magazzini automatizzati possono

finire nel mirino degli hacker, con il rischio di **furto di dati, blocchi operativi o persino manipolazioni** che mandano in tilt interi processi produttivi.

Come contrastare il rischio?

Per evitare questi scenari, è fondamentale mettere in atto alcune misure chiave: mantenere sempre aggiornati i software, utilizzare firewall potenti, crittografare i dati sensibili e separare le reti per ridurre il rischio di propagazione degli attacchi.

Anche il personale ha un ruolo importante: serve una formazione continua su come riconoscere e gestire le minacce digitali, magari con simulazioni periodiche per testare la preparazione.

Rischio di perdita di controllo umano

Un altro rischio da tenere d'occhio è **la possibile perdita di controllo sui macchinari** da parte delle persone.

Quando si affidano decisioni importanti ai sistemi intelligenti, c'è il rischio che gli operatori non riescano a intervenire tempestivamente in caso di malfunzionamenti o situazioni critiche. *Gli algoritmi, per quanto sofisticati, seguono regole rigide e spesso non sono in grado di adattarsi a cambiamenti improvvisi o a contesti imprevisti.*

Questo limite può risultare particolarmente pericoloso in scenari dove serve flessibilità o un un occhio umano per valutare le variabili in gioco.

Un esempio concreto?

Immagina una linea di produzione automatizzata dove l'IA si occupa di monitorare i macchinari. A un certo punto, un sensore rileva un

aumento di temperatura, ma l'algoritmo lo interpreta come un dato normale e lascia che la macchina continui a lavorare. Peccato che quella variazione fosse il primo segnale di un problema serio, tipo un surriscaldamento che potrebbe portare a un guasto o, peggio, a un incendio. In una situazione del genere, un operatore umano esperto si potrebbe accorgere subito che qualcosa non va e fermare la macchina per controllarla, evitando guai più grossi.

Ecco perché è fondamentale che l'IA non lavori mai completamente da sola: per quanto sia potente, non può sostituire l'occhio di chi ha esperienza e sa riconoscere e gestire gli imprevisti.

Come contrastare il rischio?

Valutare bene il rischio durante l'uso dell'impianto e avere un buon monitoraggio di quello che succede grazie alla manutenzione.

Rischi di isolamento e tecnostress

Un altro aspetto da non sottovalutare quando si parla di intelligenza artificiale in azienda è il "**tecnostress**".

Con l'automatizzazione che penetra in ogni angolo del mondo del lavoro, gli operatori si ritrovano a dover imparare continuamente come manovrare nuove tecnologie, gestire gli aggiornamenti e, in generale, affrontare un livello di connessione sempre più elevato e costante. Questo può portare a sentirsi sopraffatti, con un aumento dello stress che può avere effetti negativi sulla produttività e la salute mentale. A ciò si aggiunge anche che l'adozione massiccia delle tecnologie riduce ulteriormente le interazioni umane in fabbrica, creando un senso di **isolamento sociale** che non aiuta certo il benessere psicologico.

Come contrastare il rischio?

Come spesso accade, la chiave sta nella formazione. I lavoratori devono essere preparati non solo sui vantaggi delle nuove tecnologie, ma anche sui loro limiti e sui rischi che comportano, incluso l'impatto psicologico. Le aziende dovrebbero quindi puntare su **corsi che sensibilizzano i dipendenti** a un uso sicuro e responsabile dell'IA, ma anche sulla cybersicurezza e sulla gestione di situazioni impreviste.

È fondamentale che i lavoratori abbiano anche l'opportunità di familiarizzare con i nuovi sistemi attraverso sessioni pratiche, così da saperli usare al meglio e, se necessario, intervenire subito quando qualcosa non va.

4 Responsabilità giuridiche e intelligenza artificiale: chi risponde degli errori?

Sulla carta, usare l'intelligenza artificiale nei macchinari porta solo vantaggi. Dopotutto le IA processano molte più informazioni di quanto possa fare il nostro cervello, non sono mai stanche, non si distraggono. Eppure anche le intelligenze artificiali sbagliano, e questi errori possono portare a conseguenze molto gravi: infortuni, danni ambientali...

Ma in questi casi, su chi ricade a livello giuridico la responsabilità dell'errore? Insomma, chi finisce a processo?

Ho provato a parlare con Silvia Zuanon, avvocato d'impresa. Ne sono nate riflessioni molto interessanti, che provo ad esporre qui sotto.

Normativa sull'intelligenza artificiale: uno scenario ancora in evoluzione

L'abbiamo già accennato: il panorama normativo sull'intelligenza artificiale è ancora in piena trasformazione. **L'AI Act**, il regolamento europeo sull'intelligenza artificiale, rappresenta il primo passo concreto in questa direzione, ma ha bisogno di ulteriori norme attuative per poter diventare pienamente operativo e fare chiarezza sulle "aree grigie" di cui abbiamo discusso in precedenza.

Un altro aspetto ancora pienamente da definire riguarda proprio le responsabilità giuridiche sui danni causati dall'intelligenza artificiale. Un esempio emblematico è quello delle auto a guida autonoma: se

un veicolo investe un pedone, chi è responsabile? Il guidatore (che non guida), il produttore del sistema di intelligenza artificiale o la casa automobilistica?

Queste domande legali – ed etiche – non hanno ancora risposte definitive. Con Silvia Zuanon abbiamo tuttavia provato a rispondere, appoggiandoci alla normativa attuale e già in essere.

Responsabilità in caso di errore

Proviamo a dipingere uno scenario concreto.

Siamo in una fabbrica, e il manutentore utilizza un chatbot che gli suggerisce come riparare una valvola. Il sistema fornisce un'informazione imprecisa, qualcuno si fa male.

Di chi è la responsabilità? O, meglio ancora, come si ripartiscono le responsabilità?

1) Responsabilità del datore di lavoro

Come sempre accade nel nostro ordinamento, il datore di lavoro è in prima linea rispetto alle responsabilità legate ad un infortunio.

Il Testo Unico 81/08 ci ricorda infatti che **il datore di lavoro è generalmente responsabile per la salute e sicurezza dei lavoratori,** a meno che non possa dimostrare di aver adottato tutte le misure di prevenzione necessarie.

Nel caso specifico di un macchinario che utilizza l'intelligenza artificiale, è responsabilità del datore di lavoro:

- **Verificare la sicurezza** delle procedure generate dall'IA (la

validazione deve quindi essere un passaggio fondamentale e bloccante);

- Effettuare un'adeguata **valutazione dei rischi** legati all'utilizzo del software di intelligenza artificiale;
- Prevedere, sulla base dei rischi individuati, di **formare i lavoratori** all'utilizzo sicuro di quell'intelligenza artificiale.

Nel corso di un processo penale, dunque, il datore di lavoro può escludere la propria responsabilità se riesce a dimostrare di aver implementato tutte le misure di sicurezza e aver fornito la formazione e l'addestramento necessari ad evitare un uso improprio del macchinario da parte del lavoratore.

In linea di massima, insomma, vigono le stesse indicazioni di prevenzione e controllo del rischio che si mettono in atto per qualsiasi altro macchinario industriale.

2) Responsabilità del lavoratore nell'utilizzo delle tecnologie

In linea con l'orientamento giurisprudenziale in materia di sicurezza sul lavoro, il lavoratore tende ad essere ritenuto responsabile di un incidente o di un infortunio solo se adotta un **"comportamento abnorme"**, ossia se agisce in maniera imprudente, negligente o in violazione delle istruzioni ricevute.

È fondamentale, quindi, che le aziende forniscano un'adeguata formazione e procedure chiare, documentando le istruzioni fornite nelle sessioni di formazione. In caso contrario, il datore di lavoro può incontrare difficoltà nel dimostrare che il lavoratore ha effettivamente agito in modo contrario alle indicazioni.

Questi principi sono già consolidati nella giurisprudenza della sicurezza sul lavoro. Per il momento non ci sono novità sostanziali legate all'ambito dell'IA, ma la strada resta aperta a ulteriori sviluppi

giurisprudenziali o all'introduzione di nuove direttive specifiche.

3) Responsabilità della software house

Più interessante, forse, è capire che responsabilità assume la software house che sviluppa il sistema di intelligenza artificiale.

Partiamo da una constatazione: **le grandi tech company**, che solitamente hanno sede negli Stati Uniti, si proteggono inserendo nei contratti **solide clausole di esclusione di responsabilità**.
In pratica, è davvero difficile portare a processo queste multinazionali e riuscire ad ottenere qualcosa, anche se in Europa le normative sulla sicurezza dei prodotti impongono al produttore di rispondere in caso di lesioni o danni derivanti dal malfunzionamento del prodotto, specialmente con danni molto gravi.

Qui però dobbiamo iniziare a parlare delle software house nostrane. Nel contesto europeo, abbiamo infatti molte **software house "local"** che sviluppano applicazioni personalizzate basate su motori di IA forniti da terze parti (spesso americane).

Riprendendo il nostro esempio di partenza, possiamo supporre che una software house italiana abbia sviluppato il chatbot di assistenza installato nel macchinario. Questo chatbot è basato su uno dei grandi modelli generali di intelligenza artificiale – chat GPT, Gemini eccetera – sviluppato da aziende con sede negli USA.

Bene, se la software house italiana apporta modifiche rilevanti e sostanziali al sistema di base, la normativa europea prevede che l'azienda italiana diventi equiparabile al produttore, nel senso che ne assume le responsabilità giuridiche.

La software house locale potrà dunque essere considerata responsabile se:

- Il software fornito contiene **difetti o errori** che lo rendono non conforme alle normative di sicurezza applicabili (es. Regolamento Macchine o standard EN per la sicurezza);
- La software house non ha fornito una **documentazione adeguata** o ha omesso di informare l'utilizzatore sui rischi connessi all'uso del software;
- **Il software è stato specificatamente progettato per la macchina** e i difetti della procedura sono imputabili al software stesso.

Al contrario, la software house potrebbe escludere una propria responsabilità se riesce a dimostrare di aver rispettato gli obblighi contrattuali, normativi e tecnici, o che non aveva il controllo sull'uso improprio o scorretto del software da parte dell'utilizzatore.

Ricapitolando quanto detto finora, quali sono i diversi scenari possibili per quanto riguarda la distribuzione delle responsabilità in un infortunio legato all'uso dell'intelligenza artificiale?

- *La software house* può essere considerata responsabile se il danno deriva direttamente da un difetto del software o dalla mancanza di informazioni sui rischi;
- *Il datore di lavoro* è considerato responsabile nella maggior parte dei casi per non aver garantito la sicurezza, a meno che dimostri di aver adottato tutte le misure necessarie;
- *Il lavoratore* potrebbe essere considerato responsabile solo in casi di dolo o colpa grave, purché non riconducibile a mancanze del datore di lavoro.

Responsabilità in caso di danni a terzi

Un altro punto critico è la questione della responsabilità in caso di danni causati a terzi dall'intelligenza artificiale. Non parliamo necessariamente di una persona che si fa male, ma danni di tipo economico o anche di tipo ambientale.

Come già detto, la regolamentazione attuale è ancora in evoluzione e si attendono direttive europee più specifiche (di cui una proprio su questa tematica) per chiarire ulteriormente la divisione delle responsabilità. *Nel frattempo, si applicano i principi giuridici esistenti.*

Proviamo ad analizzare insieme le varie casistiche.

Prodotto difettoso

Se il danno è causato da un difetto del prodotto, come ad esempio un algoritmo mal progettato, e l'intelligenza artificiale è integrata in quel prodotto, ci potrebbero essere i presupposti per qualificare il prodotto come difettoso.

In questo caso si applica **la normativa sulla responsabilità per i prodotti difettosi** – la stessa che verrebbe chiamata in causa, se, ad esempio, un telefono esplodesse mentre lo si usa.

Le aziende sono già preparate a questa eventualità, in quanto tutti i produttori di beni fisici sono tenuti a dotarsi di un'assicurazione per la responsabilità civile relativa ai prodotti difettosi.

Utilizzo improprio

Se un'azienda utilizza un sistema di intelligenza artificiale **senza seguire le istruzioni del fornitore o senza effettuare una supervisione adeguata**, essa può essere considerata responsabile dei danni da esso causati. Qui entra in gioco, infatti, quel che si diceva prima

sulle procedure di validazione e sull'analisi dei rischi da effettuare sul software di IA.
Facciamo un esempio.

Utilizzi un software con un margine d'errore dichiarato dell'80%? Non puoi certo trattarlo come se il margine di errore fosse del 5%! Le procedure di supervisione e controllo devono essere estremamente più severe!

Anche la mancata adozione di misure di prevenzione, prima tra tutte **la valutazione dei rischi,** può comportare responsabilità – come ci dice la normativa relativa alla sicurezza sul lavoro.

Insomma, per aiutarti ad entrare meglio nell'ottica giusta potrebbe essere utile considerare l'intelligenza artificiale come un qualcosa di intrinsecamente pericoloso.

Per dirlo con un esempio, pensa di essere il gestore di un luna park. All'interno del parco ci sono delle giostre che, per loro natura, comportano dei pericoli. Tu che possiedi il luna park sai benissimo che devi adottare tutte le precauzioni per combattere i rischi, e sai anche che devi essere in grado di dimostrare la tua attività di prevenzione e mitigazione dei rischi in caso di necessità. Ecco, lo stesso ragionamento si potrebbe applicare a chi usa in azienda l'intelligenza artificiale.

In questo momento alcune compagnie assicurative si stanno già attivando per offrire **polizze specifiche** per coprire i rischi legati all'uso dell'intelligenza artificiale. In futuro queste protezioni assicurative potrebbero persino diventare obbligatorie, seguendo il modello delle assicurazioni su auto e veicoli. Tutto questo, però, solo il tempo potrà dircelo.

Responsabilità dell'AI e contratti: attenzione alle clausole

Partiamo da una constatazione: l'intelligenza artificiale si basa sull'analisi statistica di grandi volumi di dati. Tuttavia, quando i dati a disposizione sono insufficienti, emergono rischi significativi. Penso soprattutto a settori come l'oil and gas, dove errori nei piani di manutenzione gestiti dalle AI possono causare disastri ambientali (ed economici).

Il problema è che, in molti casi, i fornitori di soluzioni AI promettono risultati eccezionali, ma non dichiarano esplicitamente **i limiti** dei loro sistemi – perlomeno non nella fase di proposta commerciale. Tuttavia questi limiti inficiano sulla capacità predittiva delle IA, e potrebbero portare a danni imprevedibili, mettendo a rischio chi ha adottato la soluzione.

Ecco perché chi adotta soluzioni di intelligenza artificiale in azienda deve prestare molta attenzione ai contratti, in particolare alle **clausole contrattuali** che le software house inseriscono per escludere la loro responsabilità in caso di danni. Queste clausole sono spesso difficili da eliminare o negoziare, soprattutto se il fornitore è di grandi dimensioni e ha un forte potere contrattuale.

In alcuni casi, le clausole di limitazione di responsabilità vengono esplicitamente indicate come **clausole vessatorie**. Sono, tipicamente, quelle poste in fondo al contratto, scritte in piccolo...

Ecco, io dico sempre di leggere i contratti di vendita integralmente e con attenzione. Ma, se proprio non lo vuoi fare, almeno leggiti bene le clausole vessatorie!!

Per riassumere

L'abbiamo già detto in tutti i modi, ma vale la pena ripeterlo: ci troviamo in un'epoca di transizione, una terra di mezzo in cui le normative specifiche sull'intelligenza artificiale sono ancora in via di sviluppo.

Nonostante ciò, le aziende possono trovare dei punti di riferimento nelle norme già presenti: la legislazione sulla sicurezza del lavoro, le norme del codice civile o la legislazione sulla responsabilità per prodotti difettosi.

È evidente, tuttavia, che è necessaria una regolamentazione più chiara, in grado di definire in modo univoco responsabilità e requisiti di sicurezza per i sistemi di AI. Speriamo che le norme su cui si sta lavorando a livello europeo possano venirci in aiuto in questo senso.

Nel frattempo, come dovrebbero muoversi le imprese? Tre sono, a mio parere, i punti chiave:

- Valutazione attenta dei rischi legati all'IA e impostazione di procedure per gestire o limitare tali rischi;
- Controllo accurato dei contratti di vendita per capire esattamente le responsabilità che si assumono;
- Valutazione di coperture assicurative per gestire eventuali danni a cose e persone.

Solo attraverso un'attenta gestione di questi punti sarà possibile sfruttare appieno le potenzialità dell'intelligenza artificiale, minimizzando i rischi legali e operativi.

5 Intelligenza artificiale e trattamento dei dati sensibili (GDPR)

Quando si parla di intelligenza artificiale nelle fabbriche, spesso si sottovaluta un aspetto importante: **il trattamento dei dati sensibili**, e le ricadute rispetto al **GDPR** (Regolamento generale sulla protezione dei dati).

È noto che sistemi come i software AI per la diagnostica medica trattano dati sensibili, e che anche software come chat GPT possono avere a che fare con dati personali. Si tende però a pensare che nelle fabbriche questo problema non ci sia.

Ma è davvero così?

Non esattamente. Pensiamo ad esempio ad un software di AI che aiuta a organizzare l'addestramento e la formazione degli operai. Nel sistema potrebbero essere inseriti dati personali come nomi e cognomi, codici fiscali...

Oppure, ancora, pensiamo ai DPI che rilevano parametri vitali come il battito cardiaco, la temperatura corporea, la saturazione dell'ossigeno o l'elettrocardiogramma per monitorare che gli operatori non siano vittime di incidenti. Questi sono certamente dati sensibili!

Un altro esempio può venire dal mondo dei produttori di macchinari, che possono decidere di integrare un chatbot di assistenza personalizzata nella macchina. Anche questo chatbot potrebbe richiedere i dati personali della persona con cui si interfaccia (almeno nome e cognome).

Cosa succede poi a quei dati? Vengono effettivamente trattati e conservati ai sensi del GDPR?

Proviamo a capire quali sono le domande da porsi per rispettare la legge, aiutandoci anche qui con le preziose indicazioni dell'avvocato Silvia Zuanon.

Intelligenze artificiali e protezione dei dati sensibili: legittimità del trattamento

La prima domanda da porsi è: i dati forniti ai sistemi di AI possono essere trattati legalmente?

Secondo il GDPR, il trattamento di dati personali è lecito solo se esiste una base giuridica valida, come il consenso dell'utente, l'adempimento di un contratto o il legittimo interesse del titolare del trattamento.

Facciamo un esempio.

Sei un'azienda che fornisce un servizio di assistenza e metti a disposizione un chatbot per rispondere o almeno scremare le richieste. In questo caso il trattamento dei dati è considerato lecito in quanto stai adempiendo ad un contratto. In altre parole, i dati servono per poter offrire il servizio che metti a disposizione.

Tra parentesi, questo discorso vale per ogni tipologia di trattamento dati: anche se inserisci dei nominativi nel gestionale aziendale hai degli obblighi legati al GDPR. Nel caso delle intelligenze artificiali, però, il trattamento è automatizzato. *È quindi necessario informare l'utente al momento della raccolta dei dati e specificare che essi potrebbero essere elaborati anche tramite intelligenza artificiale.*

Trasferimento dei dati sensibili verso server di terze parti e verso altri Paesi

Un altro aspetto cruciale da considerare è: **dove vengono conservati i dati?** I dati finiscono solo sul gestionale interno dell'azienda o vengono inviati su un server esterno?

Molto spesso la risposta è la seconda: i dati finiscono su un server esterno, dove restano per 30 giorni e poi vengono (in teoria) cancellati.

Ma se i dati finiscono su server esterni sorgono ulteriori obblighi di conformità, specialmente se i server sono situati fuori dall'UE. *Tuttavia, le aziende spesso non sanno dove si trovano i server o come i dati vengano realmente trattati!*

Se questi server non sono situati in Europa, e sono ad esempio negli Stati Uniti, il rischio di violazioni aumenta. Diventa allora fondamentale adottare misure contrattuali e tecniche per garantire la conformità al GDPR.

Ad esempio, se un'azienda utilizza un sistema di intelligenza artificiale sviluppato da un fornitore esterno all'Unione Europea, come accade di solito, l'azienda dovrebbe stipulare un accordo di nomina del fornitore come responsabile esterno del trattamento, specificando i limiti e le modalità di utilizzo dei dati.

Quando un'azienda affida a terzi il trattamento dei dati personali, entra infatti in gioco la **nomina del responsabile esterno al trattamento dati.** Questo processo implica la redazione di un accordo formale o di un atto di nomina, in cui il responsabile esterno si impegna a rispettare precise regole stabilite dal titolare del trattamento, come previsto dal Regolamento Generale sulla Protezione dei Dati (GDPR). Tali regole garantiscono che il trattamento dei dati resti conforme alle normative in vigore, proteggendo i diritti delle persone coinvolte.

Il contratto formale che designa le parti terze come responsabili del trattamento dati dovrà:

- Definire chiaramente come i dati verranno trattati;
- Garantire la conformità del fornitore al GDPR;
- Prevedere l'adozione di misure tecniche e organizzative adeguate.

Inoltre, se il server di appoggio si trova in un Paese al di fuori dell'Unione Europea, bisognerà verificare che la normativa del Paese in questione offra garanzie adeguate. Ciò avviene attraverso **accordi internazionali**, che certificano che il livello di protezione dei dati è equivalente a quello europeo.

In sintesi: a cosa fare attenzione

I rischi più comuni legati al trattamento di dati sensibili da parte dell'AI sono:

- **Dati personali inseriti in AI pubbliche o non controllate** – se l'AI non offre garanzie sul trattamento dei dati, questo potrebbe rappresentare una violazione del GDPR.
- **Condivisione non autorizzata con terzi** – è fondamentale sapere dove i dati vengono conservati e chi vi ha accesso.
- **Trattamento non trasparente**: gli interessati devono sempre sapere come e perché i loro dati vengono usati.

Tutti questi rischi possono essere bilanciati: la normativa sul trattamento dei dati prevede delle soluzioni che si possono adottare per contrastarli. Prima di tutto occorre però essere consapevoli dei pericoli, in modo da trovare poi le strategie giuste per affrontarli.

6 Un caso specifico: i chatbot per l'assistenza tecnica che usano l'IA

Fino a qui abbiamo analizzato il quadro generale. Ora proviamo a concentrarci su un caso più concreto e particolare: quello dei chatbot per l'assistenza tecnica che utilizzano l'intelligenza artificiale.

Attualmente, i software di questo tipo sono di due categorie: alcuni estraggono informazioni da vari documenti e creano link consultabili, mentre altri raccolgono ed elaborano i contenuti per generare riassunti o testi sintetici. In questo contesto ci concentreremo più sul secondo tipo di software, quelli che fanno un uso più "avanzato" dell'intelligenza artificiale.

Premessa: i vantaggi dei chatbot di assistenza che usano l'IA

Da dove nasce l'esigenza di usare l'intelligenza artificiale per i manuali dei macchinari industriali? Quali vantaggi presentano i chatbot intelligenti ?

È presto detto. Spesso i clienti, i collaboratori e i responsabili delle aziende non hanno un accesso comodo e veloce alle informazioni tecniche dei macchinari, anche perché di frequente tali informazioni non sono ben strutturate.

Sì, certo, le aziende produttrici di macchinari forniscono ormai regolarmente PDF o altri materiali online. Ma, se non si conosce esattamente la parola chiave da cercare, è facile perdere di vista informazioni utili, arrivando addirittura a credere che non esistano

soluzioni al proprio problema (anche quando non è così).

Diciamolo in un altro modo. Quando un cliente acquista un macchinario, spesso riceve una quantità esagerata di PDF con nomi poco chiari, che rendono difficile trovare le informazioni necessarie. Il problema si aggrava se vengono utilizzati termini tecnici o se i manuali sono tradotti approssimativamente da un'altra lingua. Inoltre, il cliente ha spesso in mano molteplici manuali forniti dai diversi produttori, che solitamente finiscono in archivio e non vengono mai davvero consultati.

È qui che entra in gioco l'intelligenza artificiale. Grazie alla ricerca semantica, l'IA riesce a cercare informazioni in testi non strutturati usando il linguaggio naturale. In pratica – e senza entrare troppo nei dettagli tecnici – i motori di ricerca integrati in questi software consentono di porre una domanda senza conoscere perfettamente i termini esatti utilizzati nei manuali. Il software confronta le domande con i contenuti del database aziendale e fornisce un insieme di risposte rilevanti che vengono poi elaborate e presentate all'utente, spesso tramite chatbot. Questo processo consente di trovare rapidamente informazioni anche a partire da grandi quantità di dati.

Facciamo un esempio concreto. Un manutentore ha un dubbio su una macchina. Invece di cercare manualmente tra una valanga di PDF, può porre la domanda direttamente al chatbot, che confronterà la domanda con le informazioni disponibili nel database e restituirà la risposta più utile. Chiaro, no?

Un chatbot aziendale può quindi essere estremamente utile per:

- Ridurre i tempi di risposta alle domande più frequenti, come nelle classiche FAQ;
- Facilitare l'accesso a informazioni tecniche non strutturate;

- Creare una bozza di procedure tecniche, partendo da un estratto delle informazioni più rilevanti.

Inoltre, è possibile profilare le risposte in base al tipo di utente (cliente, manutentore, ecc.), migliorando l'efficacia delle risposte e limitando i rischi.

I rischi specifici

Come abbiamo visto, l'uso dell'AI nelle fabbriche presenta ancora numerose sfide, e si porta dietro tutta una serie di rischi specifici da prendere in considerazione. Nel caso dei chatbot di assistenza tecnica, i pericoli più rilevanti sono probabilmente quelli legati alle traduzioni imperfette e alle allucinazioni dell'intelligenza artificiale. Vediamoli meglio insieme.

1. Traduzioni imperfette

Questo problema si pone soprattutto quando il software fa riferimento a manuali tecnici scritti in altre lingue o, caso più frequente, quando l'IA stessa è stata addestrata in una lingua diversa dall'italiano e fa semplicemente una traduzione automatica dall'inglese.

La traduzione automatica del chatbot è spesso approssimativa, soprattutto con i termini tecnici, anche se può comunque aiutare a far comprendere il significato generale del testo. Consideriamo anche che lo stesso componente potrebbe avere nomi diversi a seconda della filiera in cui viene utilizzato, oppure avere un nome specifico in italiano a fronte di un nome più generico in inglese.

Vero è che la qualità della traduzione dipende molto dal modello linguistico scelto per l'IA: GPT, ad esempio, ha ottime capacità perché è stato addestrato su testi da tutto il mondo e migliora nel tempo. In ogni caso, questa dinamica crea rischi di fraintendimento di cui bisogna tenere conto.

2. Allucinazioni dell'AI

Abbiamo già accennato al fenomeno delle allucinazioni dell'intelligenza artificiale, per cui l'IA genera risposte che sembrano logiche e verosimili, ma basandosi su supposizioni errate e non su dati reali. Questo avviene perché i modelli linguistici delle IA elaborano testi in base a probabilità statistiche, non necessariamente a fatti concreti.

Ma quando parliamo di procedure di utilizzo, manutenzione e sicurezza dei macchinari, le allucinazioni possono essere davvero pericolose!

Facciamo degli esempi pratici. Immaginiamo che un macchinario si blocchi, segnalando il codice di errore E57. Il tecnico chiede supporto al chatbot di assistenza, che risponde:

L'errore E57 indica un surriscaldamento del motore principale. Per risolvere il problema, spegni la macchina, smonta il pannello del motore e sostituisci la scheda di controllo interna.

Il tecnico, fidandosi del chatbot, segue le istruzioni. Tuttavia, il codice errore E57 si riferisce in realtà a un semplice problema di sensore. Smontare il pannello e manipolare la scheda di controllo non solo è inutile, ma provoca un danno alla macchina, aumentando i tempi di inattività e i costi di riparazione.

Altro caso, questo un po' più estremo. Il braccio robotico del macchinario è bloccato. Il manutentore chiede al chatbot come intervenire e questo gli risponde di disattivare il blocco di emergenza e riattivare manualmente il braccio. Peccato che appena il tecnico interviene, quello si muove improvvisamente, rischiando di colpirlo e fargli davvero molto male. Il classico avvio inatteso.

Per mitigare questi rischi, è fondamentale che il chatbot si basi sulla specifica knowledge base aziendale (manuali, contenuti interni) e non solo sul database del modello GPT generale. Il sistema deve essere istruito a generare risposte precise, basate solo sui dati aziendali, e a citare sempre le fonti. Ad esempio, se il chatbot suggerisce come usare una macchina, dovrà fornire un link al manuale originale per verifica.

Bisogna inoltre impostare delle ferree procedure di validazione umana con le quali dare il via libera finale alle azioni suggerite dai chatbot. Anche l'addestramento degli operatori andrà impostato in tal senso: se non si rendono chiare le limitazioni del software, si rischia infatti anche che i tecnici perdano fiducia quando si verifica un'allucinazione, e finiscano per non evitare del tutto l'utilizzo del chatbot!

Tiriamo le somme

Le aziende stanno sempre più utilizzando chatbot per migliorare l'assistenza clienti e l'assistenza tecnica e per gestire meglio le informazioni interne. Non si tratta, quindi, di strumenti ipotetici, ma di tecnologie che sono già qui tra noi, in uso.

Alcuni chatbot aziendali possono essere configurati per fornire risposte personalizzate in base al tipo di utente (es.utenti generici o manutentori) attraverso sistemi di login e metadati. Ad esempio, un utente generico potrebbe ricevere "informazioni di base" su un macchinario, mentre un tecnico riceverà dettagli specifici e istruzioni più complesse. Questa divisione dei ruoli permette di rendere il chatbot uno strumento utile sia per chi cerca informazioni preliminari sia per chi deve intervenire operativamente sulla macchina, e minimizza alcuni dei rischi collegati all'utilizzo del software.

Un altro vantaggio di questi prodotti è che i chatbot possono essere usati per rispondere a domande ripetitive che vengono fatte frequentemente, un po' come una versione evoluta delle FAQ. Quando un cliente pone una domanda comune, il chatbot può cercare tra i documenti aziendali e fornire una risposta rapida e precisa, riducendo il numero di chiamate all'assistenza tecnica. Per esempio, se molte persone chiedono informazioni simili su una macchina, il chatbot può recuperare e restituire sempre la stessa risposta validata. Questo rende il processo più efficiente e riduce il carico sugli uffici tecnici.

Tuttavia, il sistema non è infallibile. Esiste il rischio che il chatbot non trovi una risposta nella knowledge base aziendale, oppure che la risposta non sia aggiornata o completa. In questi casi, la domanda dell'utente diventa un'opportunità per l'azienda che fornisce il supporto tecnico: raccogliere queste richieste non risolte permette di migliorare costantemente il database di conoscenze e ridurre la dispersione di informazioni. Questo è fondamentale, perché molte aziende ignorano le domande irrisolte o non si rendono conto che i loro clienti stanno cercando informazioni che non sono facilmente reperibili.

Inoltre, un chatbot avanzato può interfacciarsi con tecnologie che convertono testo in voce, migliorando ulteriormente l'accessibilità e l'efficienza del sistema.

Il timore principale nell'implementazione di un chatbot di assistenza tecnica è che possa fornire informazioni imperfette, portando a una perdita di fiducia da parte degli utenti. Per evitare questo, è consigliabile implementarlo gradualmente. Si può iniziare con un uso interno, validare le informazioni passo dopo passo e solo successivamente estenderlo ai clienti. La costruzione della fiducia è un processo graduale, e partire da un approccio lento ma costante è sicuramente il metodo più indicato.

APPROFONDIMENTO A CURA DI

Silvia Zuanon

Avvocato d'impresa

L'AI ACT, SPIEGATO SEMPLICE

Il regolamento (UE) 2024/1689, noto come AI Act, introduce una normativa europea organica sull'intelligenza artificiale, mirata a bilanciare la protezione dei diritti e delle libertà dei cittadini dell'Unione con il supporto all'innovazione tecnologica. Le disposizioni principali sono entrate in vigore il **2 febbraio 2025**, vietando specificamente l'uso di IA che manipolano comportamenti subliminali, classificano persone in base al "punteggio sociale" o predicono comportamenti criminali attraverso profilazione della personalità. Sono proibiti anche i sistemi che analizzano le emozioni in ambito lavorativo o educativo e le banche dati di riconoscimento facciale raccolte in massa da fonti pubbliche. Le sanzioni per le infrazioni possono arrivare fino a 35 milioni di euro o al 7% del fatturato globale delle aziende non conformi.

Dal **2 agosto 2027** scatteranno ulteriori obblighi per i sistemi di IA ad alto rischio, come quelli operanti in settori critici (infrastrutture, sanità, istruzione) o impiegati per l'identificazione remota, con sanzioni fino a 15 milioni di euro o il 3% del fatturato. Tra queste date sono previste scadenze per l'adeguamento di tecnologie quali i modelli di IA generativa (ad es. Chat GPT).

Il regolamento richiede che le imprese operanti con IA inizino a prepararsi, familiarizzando con le regole e adottando misure di conformità, anche se ad oggi mancano linee guida e modelli operativi dettagliati. Le imprese dovranno inoltre confrontarsi con altre normative, come GDPR e Digital Service Act, per essere pienamente conformi.

I principi dell'AI Act

L'AI Act dell'Unione Europea, frutto di quattro anni di lavoro, stabilisce una cornice normativa unica al mondo per regolamentare l'intelligenza artificiale (IA) nel mercato interno, favorendo un approccio antropocentrico e affidabile. Il regolamento mira a proteggere diritti fondamentali come salute, sicurezza, democrazia, Stato di diritto e ambiente, bilanciando prevenzione dei rischi e promozione dell'innovazione.

L'approccio antropocentrico pone l'essere umano al centro delle decisioni prese dai modelli IA: l'uomo deve poter mantenere il controllo su decisioni in settori sensibili, riducendo al minimo il rischio di effetti nocivi. La trasparenza è un pilastro dell'AI Act, imponendo che i modelli IA siano progettati per consentire di tracciare il processo decisionale, requisito complesso per modelli avanzati e addestrati su grandi volumi di dati.

Inoltre, **il concetto di "affidabilità"** si traduce in requisiti di sicurezza informatica, robustezza e resilienza: i sistemi devono produrre risultati stabili con input simili e gestire i dati in modo sicuro. Tuttavia, fenomeni come le "allucinazioni" dei modelli linguistici, risposte apparentemente sensate ma errate, pongono ancora sfide di trasparenza.

Il regolamento segue **un approccio basato sul rischio**, classificando i sistemi IA in rischio inaccettabile (vietato), alto rischio (sottoposto a norme specifiche) e rischio basso o nullo. I sistemi ad alto rischio includono applicazioni critiche, come quelle sanitarie o infrastrutturali, e sono soggetti a obblighi rigorosi di trasparenza e tracciabilità. Altri sistemi richiedono semplicemente la trasparenza delle loro operazioni, ma con minori vincoli.

L'AI Act rappresenta quindi un regolamento che, come il GDPR per la privacy, ha una funzione protettiva e incentivante: l'obiettivo è creare un quadro normativo stabile e certo, in cui le aziende possano operare senza incertezze normative, mentre i consumatori possono affidarsi alla tecnologia sapendo che è sicura e rispettosa dei loro diritti fondamentali.

Disposizioni generali dell'AI Act

Questo capitolo del regolamento, costituito da quattro articoli, chiarisce a quali soggetti e ambiti si applichi l'AI Act e contiene le definizioni chiave per la sua interpretazione.

L'Articolo 2 stabilisce che il regolamento non si applica a sistemi di IA open source (salvo eccezioni), a quelli utilizzati per scopi scientifici, né a sistemi impiegati per difesa e sicurezza nazionale. In sintesi, le aziende che producono, utilizzano o distribuiscono IA per scopi commerciali devono osservare questa normativa, mentre sistemi in contesti militari, di sicurezza o di ricerca ne sono generalmente esenti.

L'Articolo 3, cruciale per la comprensione del regolamento, definisce 68 termini fondamentali, includendo i ruoli di "fornitore", "deployer", "importatore" e "distributore". Il fornitore è chi sviluppa

o commercializza un sistema di IA, assumendosi la responsabilità anche se non ne ha curato la realizzazione tecnica, purché apponga il proprio marchio sul prodotto. Il deployer è l'utilizzatore del sistema di IA, a cui si attribuiscono responsabilità specifiche se apporta modifiche sostanziali al sistema. Gli importatori e distributori, invece, immettono o distribuiscono il sistema sul mercato dell'Unione Europea, con obblighi di conformità variabili in base al loro ruolo.

La definizione di "sistema di IA" è un altro punto focale: viene descritto come un sistema automatizzato che opera con vari gradi di autonomia e può adattarsi post-distribuzione per generare output (come previsioni o raccomandazioni) che influenzano ambienti fisici o virtuali. Questa definizione si distingue dalle semplici analisi statistiche per via dell'adattabilità del sistema, il che implica la capacità di evolversi basandosi sull'esperienza. Un sistema di IA, dunque, non è solo in grado di generare output da input come un programma statistico, ma può modificare le sue risposte nel tempo, in funzione delle nuove informazioni apprese.

È interessante notare che un modello di IA con parametri rigidi, che non evolve, potrebbe non rientrare in questa definizione e quindi non essere considerato IA secondo il regolamento. Questa distinzione può richiedere chiarimenti applicativi per stabilire con precisione quali modelli siano soggetti alla norma.

L'Articolo 4, infine, introduce un obbligo di alfabetizzazione in materia di IA per i fornitori e deployer, che devono garantire che il proprio personale (o chiunque utilizzi i sistemi di IA per loro conto) sia adeguatamente informato sui meccanismi e sui rischi legati all'IA. Questo obbligo formativo deve essere documentato e rappresenta una responsabilità specifica per le imprese, che

devono dunque predisporre procedure informative per garantire la consapevolezza e la sicurezza nell'uso di tali tecnologie.

In sintesi, questo capitolo dell'AI Act si occupa di definire l'ambito della normativa, chiarendo ruoli e responsabilità di chi sviluppa, utilizza o commercializza sistemi di IA. La norma si concentra su sistemi adattivi e con autonomia decisionale, imponendo alle imprese non solo il rispetto di criteri tecnici, ma anche l'obbligo di fornire una conoscenza adeguata ai loro operatori.

Pratiche vietate

Il Capo II, composto dall'unico articolo 5, elenca le pratiche vietate per i sistemi di IA. Le imprese devono verificare attentamente se i loro sistemi rientrano in queste categorie vietate, poiché l'AI Act mira a impedire usi considerati dannosi o lesivi dei diritti. I sistemi di IA proibiti includono quelli che:

- Usano tecniche subliminali manipolative per influenzare inconsapevolmente il comportamento delle persone;
- Sfruttano vulnerabilità di specifici gruppi (come anziani o disabili) per manipolare comportamenti;
- Assegnano un "punteggio sociale" che può causare discriminazioni;
- Profilano le persone per prevedere comportamenti criminali (polizia predittiva);
- Creano banche dati di riconoscimento facciale tramite scraping indiscriminato di immagini online o da videocamere;
- Analizzano le emozioni in ambiti lavorativi o educativi;
- Inferiscono caratteristiche biometriche legate a razza, orientamento politico o religioso, sessualità, o affiliazione sindacale.

L'articolo 5 vieta anche l'uso di sistemi di identificazione biometrica remota in tempo reale in spazi pubblici, salvo eccezioni specifiche, come nel caso di ricerche per persone scomparse o nel contrasto a tratta di esseri umani. In tali contesti, il regolamento cerca di bilanciare privacy e sicurezza, limitando l'uso di tali sistemi a scopi di protezione e legalità.

Per le imprese, una lettura dettagliata dell'articolo 5 e dell'allegato II è essenziale, poiché definiscono chiaramente i limiti d'uso per sistemi IA potenzialmente invasivi, garantendo che queste tecnologie non violino diritti fondamentali o privacy individuale.

Sistemi ad alto rischio

Il Capitolo III dell'AI Act, uno dei più rilevanti per le aziende, tratta delle disposizioni per i sistemi di intelligenza artificiale considerati "ad alto rischio." Comprende 44 articoli suddivisi in varie sezioni:

1. **Classificazione dei sistemi ad alto rischio**
   L'articolo 6 identifica i sistemi di IA "ad alto rischio," rimandando agli Allegati I e III, che elencano settori e contesti d'uso specifici. L'Allegato I definisce ambiti già regolati da normative UE per sicurezza e conformità, come dispositivi medici e attrezzature di sicurezza. L'Allegato III riguarda nuovi ambiti in cui l'IA è rilevante, come biometria, infrastrutture critiche, educazione, occupazione, servizi essenziali, e attività di contrasto. I sistemi IA in questi contesti vengono classificati ad alto rischio, se utilizzati per applicazioni specifiche come l'identificazione biometrica, la valutazione del rischio lavorativo, o l'assistenza giudiziaria. Inoltre, alcuni sistemi possono essere considerati a rischio inferiore se eseguono solo compiti limitati o preparatori e lasciano la decisione

finale a un essere umano.

2. **Requisiti per i sistemi ad alto rischio**
   Gli articoli dall'8 al 15 specificano requisiti per i sistemi IA ad alto rischio, obbligando le imprese a garantire la gestione dei rischi, la qualità e la sicurezza dei dati di addestramento, e la trasparenza. Un sistema ad alto rischio deve essere supportato da una documentazione tecnica che dimostri la sua conformità normativa e includere una funzione di registrazione degli eventi per monitorare il comportamento del sistema. Le imprese devono assicurare che gli utenti possano comprendere il funzionamento, l'affidabilità e i limiti del sistema, con supervisione umana continua. La robustezza, l'accuratezza e la sicurezza informatica del sistema sono fondamentali, e la Commissione UE stabilirà parametri di riferimento per la conformità.

3. **Obblighi per fornitori e deployer**
   Gli articoli dal 16 al 25 dettagliano i doveri dei fornitori (coloro che immettono il sistema sul mercato), dei deployer (gli utilizzatori) e degli intermediari come importatori e distributori. I fornitori devono garantire la qualità e mantenere tutta la documentazione per dieci anni, monitorando la conformità e segnalando eventuali problemi alle autorità. Devono inoltre cooperare con le autorità e implementare un sistema di gestione della qualità che includa la progettazione del sistema, il monitoraggio dei rischi, e procedure di reportistica per incidenti. Gli importatori e distributori devono verificare che il fornitore abbia rispettato tutte le richieste del regolamento, diventando l'interfaccia tra il sistema e le autorità nazionali. L'articolo 25 introduce anche il concetto di "responsabilità lungo la catena del valore," stabilendo

che importatori, distributori o deployer possono diventare fornitori se modificano sostanzialmente il sistema o ne cambiano la finalità.

4. **Obblighi dei deployer**
   Gli articoli 26 e 27 stabiliscono gli obblighi dei deployer, cioè degli utilizzatori dei sistemi IA ad alto rischio, come adottare misure per garantire un uso conforme alle istruzioni e formare il personale sull'utilizzo sicuro del sistema. Devono monitorare continuamente il sistema, notificare rischi e incidenti, conservare i log degli eventi e informare le persone interessate. I deployer di enti pubblici, banche e assicurazioni devono anche eseguire una "valutazione di impatto sui diritti fondamentali," analizzando il potenziale impatto dei sistemi IA sui diritti delle persone coinvolte.

5. **Autorità di notifica e organismi notificati**
   Gli articoli dal 28 al 39 descrivono la costituzione delle autorità di notifica, responsabili per la designazione e il monitoraggio degli organismi di valutazione della conformità. Questi enti agiranno come certificatori, verificando che i sistemi IA ad alto rischio rispettino le normative.

6. **Norme di conformità e certificazione**
   Gli articoli dal 40 al 49 specificano le procedure per la certificazione, la registrazione e la marcatura CE dei sistemi ad alto rischio. Tuttavia, queste procedure saranno delineate più dettagliatamente quando verranno istituiti gli organismi di valutazione e le linee guida specifiche.

In sintesi, il Capitolo III impone requisiti rigorosi per i sistemi IA ad alto rischio, definendo gli ambiti applicativi, le responsabilità degli

operatori lungo la catena di distribuzione e le regole di conformità e monitoraggio. Le imprese devono predisporre documentazione dettagliata, un sistema di gestione qualità, e fornire formazione e trasparenza agli utenti, contribuendo a un utilizzo sicuro e responsabile dell'intelligenza artificiale in settori critici.

Il Capitolo III dell'AI Act, articolato in 44 articoli e cinque sezioni, stabilisce inoltre le norme fondamentali per i sistemi di IA classificati come "ad alto rischio," fornendo una struttura dettagliata di requisiti, responsabilità e controlli specifici per garantire sicurezza e conformità nei settori critici. Le aziende che sviluppano, distribuiscono o utilizzano sistemi IA devono porre particolare attenzione a queste disposizioni per evitare sanzioni e garantire che le loro tecnologie rispettino gli standard dell'Unione Europea. Di seguito, una panoramica dettagliata delle sezioni e dei requisiti stabiliti dal Capitolo III.

La Sezione 1, articolata nell'articolo 6, fornisce i criteri per identificare i sistemi di IA considerati ad alto rischio. La norma distingue i contesti in cui il rischio per i diritti e la sicurezza è particolarmente alto e fa riferimento agli Allegati I e III per stabilire le categorie specifiche.

L'Allegato I elenca settori già regolamentati nell'Unione Europea in cui sono presenti normative specifiche di sicurezza, come dispositivi medici, giocattoli, ascensori, veicoli e sistemi di protezione contro atmosfere esplosive. In questi casi, i sistemi di IA utilizzati in questi contesti devono rispettare normative stringenti già stabilite, che richiedono una valutazione della conformità da parte di terzi. L'AI Act specifica che solo se tali sistemi sono soggetti a valutazione da parte di organismi esterni, sono considerati "ad alto rischio."

L'Allegato III elenca nuovi settori emergenti che richiedono una regolamentazione specifica a causa dell'uso sempre più diffuso di IA. Tra questi si includono la biometria, le infrastrutture critiche, il settore educativo, il mercato del lavoro, i servizi essenziali e la giustizia. Per esempio, i sistemi di identificazione biometrica o di categorizzazione biometrica, i sistemi che riconoscono le emozioni nei luoghi di lavoro o nell'istruzione, e i sistemi che gestiscono infrastrutture digitali o erogano servizi pubblici, sono inclusi come ad alto rischio. Questo include sistemi di IA utilizzati per selezionare e valutare candidati, determinare la qualità dei servizi sanitari o prendere decisioni che incidono sulle condizioni di lavoro e sulle prestazioni degli individui.

L'articolo 6 prevede anche delle eccezioni per quei sistemi IA elencati nell'Allegato III che eseguono compiti limitati o preparatori e non sostituiscono la decisione umana. Quando la supervisione umana è costante e sostanziale, l'IA può essere declassificata da "ad alto rischio," rendendo così più chiaro il confine tra i sistemi soggetti alle disposizioni più severe dell'AI Act e quelli esenti.

Sezione 2: Requisiti per i sistemi ad alto rischio

La Sezione 2, che va dall'articolo 8 all'articolo 15, stabilisce requisiti fondamentali per i sistemi di IA ad alto rischio, garantendo sicurezza, trasparenza e affidabilità. Questi articoli richiedono che le aziende creino un solido **sistema di gestione dei rischi** (articolo 9), che consente di identificare e mitigare rischi associati al sistema in tutto il suo ciclo di vita. Questo sistema di gestione include l'analisi delle fasi di sviluppo, addestramento, implementazione e monitoraggio.

L'articolo 10 richiede alle aziende di adottare una gestione dei dati

rigorosa per garantire che l'IA si basi su dati accurati, rappresentativi e privi di bias. I dati utilizzati per addestramento, validazione e testing devono rispondere a standard qualitativi elevati, in modo da evitare distorsioni e discriminazioni. Per conformarsi a questa norma, le aziende devono dimostrare che i dati utilizzati siano accuratamente selezionati, privi di errori o bias che possano compromettere il corretto funzionamento del sistema IA.

L'articolo 11 impone l'obbligo di una documentazione tecnica completa che dimostri la conformità del sistema alle disposizioni dell'AI Act. Questa documentazione deve essere redatta prima che il sistema venga commercializzato o messo in servizio e mantenuta aggiornata per tutta la vita del sistema. Include anche informazioni sulla progettazione, sull'implementazione e sulle modifiche al sistema, nonché sui risultati dei test di sicurezza.

L'articolo 12 introduce il requisito di un sistema di registrazione degli eventi (log) che registri ogni operazione significativa compiuta dal sistema IA. Questa tracciabilità è essenziale per monitorare e analizzare le prestazioni del sistema nel tempo, consentendo di identificare eventuali anomalie o rischi. I log devono essere mantenuti accessibili per tutta la durata del sistema, in modo che le autorità competenti possano accedervi in caso di ispezioni o verifiche.

L'articolo 13 riguarda la comunicazione con gli utilizzatori del sistema (deployer), i quali devono ricevere informazioni dettagliate sul funzionamento del sistema, sui suoi limiti e sui rischi associati. In questo modo, gli utenti possono capire le capacità del sistema IA e utilizzarlo in modo appropriato, evitando situazioni in cui le aspettative sulle prestazioni siano sproporzionate rispetto alla realtà.

L'articolo 14 introduce l'obbligo di garantire che il sistema IA sia supervisionabile da esseri umani. La supervisione umana è essenziale per evitare situazioni in cui il sistema IA prenda decisioni in modo completamente autonomo senza la possibilità di un intervento umano in caso di errore o malfunzionamento.

Infine, l'articolo 15 richiede che il sistema IA ad alto rischio sia robusto, accurato e sicuro dal punto di vista informatico. La Commissione Europea stabilirà i parametri di riferimento per garantire che i modelli rispettino standard elevati di qualità e sicurezza.

Sezione 3: Obblighi per i fornitori e deployer di sistemi ad alto rischio

La Sezione 3, composta dagli articoli dal 16 al 25, specifica gli obblighi dei fornitori (chi sviluppa e distribuisce il sistema), dei deployer (chi lo utilizza) e degli intermediari come importatori e distributori. I fornitori sono responsabili della qualità e della conformità dei loro sistemi IA, garantendo che rispettino tutti i requisiti descritti nella Sezione 2. Devono implementare **un sistema di gestione della qualità** che include strategie di conformità, tecniche di progettazione, gestione dei dati e monitoraggio dei rischi.

I fornitori sono tenuti a conservare la documentazione relativa ai propri sistemi per almeno dieci anni e a mantenere i log per sei mesi, se sotto il loro controllo. Devono monitorare la conformità del sistema e informare le autorità in caso di problemi, ritirando il prodotto dal mercato se necessario. Inoltre, devono collaborare con le autorità di vigilanza e tenere traccia dei cambiamenti che potrebbero influenzare il funzionamento del sistema.

Gli importatori e i distributori hanno l'obbligo di verificare che i sistemi rispettino le normative e di comunicare tempestivamente alle autorità eventuali problemi. In caso di incidenti gravi o modifiche significative al sistema, diventa loro compito informare le autorità di vigilanza.

L'articolo 25 stabilisce che importatori, distributori o deployer possono diventare "fornitori" nel caso in cui apportino modifiche significative al sistema o cambino la sua finalità. Questo include l'apposizione del proprio marchio o nome sul sistema IA. Il concetto di "modifica sostanziale" sarà oggetto di chiarimenti normativi, poiché è fondamentale per stabilire le responsabilità lungo la catena di distribuzione.

Sezione 4: Autorità di notifica e organismi notificati

Gli articoli dal 28 al 39 della Sezione 4 definiscono la costituzione e i ruoli delle **autorità di notifica** e degli **organismi notificati**. Le autorità di notifica sono responsabili della designazione e del monitoraggio degli organismi di valutazione della conformità, che agiscono come enti certificatori. Questi organismi verificano che i sistemi IA ad alto rischio rispettino i requisiti del regolamento, rilasciando certificazioni di conformità e assicurando che i sistemi rispettino gli standard europei.

Questa sezione assicura che le valutazioni di conformità siano condotte da enti competenti e indipendenti, evitando conflitti di interesse e garantendo una supervisione rigorosa del processo di certificazione. Gli organismi notificati devono possedere competenze tecniche e rispettare standard elevati per garantire una valutazione accurata dei sistemi IA.

Sezione 5: Norme, valutazione della conformità, certificati e registrazione

Gli articoli dal 40 al 49 descrivono le procedure **per la certificazione, la registrazione e la marcatura CE** dei sistemi di IA ad alto rischio, sebbene molti dettagli operativi debbano ancora essere specificati quando verranno istituiti gli organismi di valutazione. La marcatura CE garantisce che un prodotto sia conforme ai requisiti dell'AI Act e può essere utilizzata solo se il sistema ha superato tutti i test di conformità richiesti.

Obblighi di trasparenza

Il Capo IV dell'AI Act, composto dal solo articolo 50, introduce obblighi di trasparenza specifici per i fornitori e deployer di determinati sistemi di IA, applicandosi a una vasta gamma di tecnologie, indipendentemente dal livello di rischio generalmente attribuito. Questo articolo si focalizza sui sistemi che interagiscono direttamente con le persone (come chatbot), che generano contenuti sintetici (audio, video, immagini, testi), riconoscono emozioni, o creano "deep fake" manipolando contenuti multimediali.

In tutti questi casi, è obbligatorio informare gli utenti finali che stanno interagendo con un prodotto generato da IA, per evitare manipolazioni o fraintendimenti. Questo obbligo mira a prevenire usi rischiosi e ingannevoli, imponendo una trasparenza anche per i sistemi non classificati ad alto rischio o vietati, poiché il legislatore riconosce il potenziale danno sociale e psicologico dei contenuti non etichettati come originati dall'IA.

Sono previste eccezioni per l'uso da parte delle autorità di contrasto o per contenuti di IA usati a fini di assistenza editoriale standard.

La Commissione Europea fornirà linee guida e incentiverà codici di buone pratiche per l'etichettatura di questi prodotti, rendendo più facile l'identificazione dei contenuti generati da IA. Tali codici, cruciali per l'industria, garantiranno un utilizzo più sicuro dell'IA. Infine, l'articolo 50 anticipa la gestione dei sistemi IA generativi, includendo i contenuti "fake" o manipolati prodotti da questi strumenti, che vengono trattati anche nel successivo Capo V.

L'IA generativa

Il Capo V dell'AI Act, diviso in 4 sezioni e composto da 6 articoli, si concentra sull'intelligenza artificiale generativa, rivolta a modelli come Chat GPT e Gemini. Questo capitolo è stato aggiunto durante il processo di definizione dell'AI Act, poiché i grandi modelli linguistici, basati su architetture avanzate come i transformer, non erano ancora sviluppati o noti per le loro capacità all'avvio dell'iter normativo nel 2021. Con l'emergere delle loro potenzialità alla fine del 2022, si è reso necessario regolare questi sistemi, che hanno una portata e un impatto significativi in ambito sociale, economico e persino politico.

Definizione dei modelli di IA per finalità generali

L'AI Act classifica l'intelligenza artificiale generativa come "modelli di IA per finalità generali," poiché tali sistemi non sono progettati per compiti specifici, ma per un'ampia gamma di applicazioni. Nell'articolo 3, punto 63, si definisce un modello di IA per finalità generali come caratterizzato da una "generalità significativa", ovvero capace di svolgere vari compiti distinti, indipendentemente dalle modalità con cui viene immesso sul mercato. Questa definizione, pur ampia, non include i modelli sviluppati per la ricerca o prototipazione prima della commercializzazione, in

quanto l'AI Act interviene solo sui modelli destinati all'uso pubblico o commerciale, salvaguardando così la ricerca.

L'ampiezza della definizione consente all'AI Act di inglobare non solo i sistemi attuali, ma anche quelli futuri, adattabili e in evoluzione. Inoltre, la legge precisa che un modello di IA rientra in questa categoria anche se è addestrato su grandi quantità di dati mediante autosupervisione, un chiaro riferimento ai modelli linguistici che usano milioni o miliardi di parametri per generare testo o rispondere a domande, come Chat GPT.

Sistemi di IA per finalità generali

Il punto 66 dell'articolo 3 introduce un'ulteriore distinzione tra modelli e sistemi di IA per finalità generali. Un "sistema di IA per finalità generali" è un sistema costruito su un modello di IA per finalità generali, ma pronto per un uso immediato e che non richiede ulteriori sviluppi o integrazioni. Questa distinzione, pur non presente per altri tipi di IA, è importante poiché comporta differenti obblighi in base alla modalità di utilizzo. Un modello di IA generativo può essere utilizzato da diverse organizzazioni, integrato in altri sistemi o direttamente impiegato per varie applicazioni senza modifiche. Tale distinzione obbliga le aziende a distinguere tra chi sviluppa il modello e chi utilizza un sistema già pronto.

Rischio sistemico e impatto elevato

Gli articoli 64 e 65 dell'AI Act descrivono i concetti di "rischio sistemico" e "impatto elevato." Il rischio sistemico si riferisce alla capacità di alcuni modelli di IA di generare effetti negativi significativi su larga scala, influenzando la salute pubblica, la

sicurezza, i diritti fondamentali o la società nel suo complesso. Questo rischio può estendersi lungo l'intera catena del valore e avere un impatto su scala globale. L'"impatto elevato" riguarda la potenza e la portata dei modelli, dove i sistemi più avanzati, come i modelli linguistici di grandi dimensioni, mostrano una potenziale capacità di generare danni o di influenzare in modo sostanziale la società.

Inoltre, l'articolo 51 introduce una classificazione aggiuntiva per i modelli di IA generativi a rischio sistemico. Questa classificazione viene applicata quando un modello presenta capacità di impatto elevato secondo valutazioni tecniche, o in base a una decisione della Commissione Europea, spesso a seguito di segnalazioni del gruppo di esperti scientifici. Questa valutazione si basa su elementi definiti nell'Allegato XIII dell'AI Act, come il numero di parametri del modello, la qualità dei dati di addestramento, la potenza di calcolo richiesta per l'addestramento e il numero di utenti che utilizzano il modello.

Per definire la soglia del rischio sistemico, l'articolo 51 stabilisce un parametro specifico: se la quantità di calcolo cumulativa utilizzata per addestrare un modello supera 10^{25} operazioni in virgola mobile, il modello viene considerato ad alto rischio. Questo parametro numerico è stato scelto come riferimento, ma la Commissione si riserva il diritto di aggiornarlo nel tempo, in base agli sviluppi tecnologici e alla crescente potenza di calcolo disponibile.

Obblighi per i fornitori di modelli generativi

Gli articoli 53 e 54 dell'AI Act stabiliscono i requisiti per i fornitori di modelli generativi. Le imprese devono fornire una documen-

tazione tecnica dettagliata per dimostrare la conformità del modello ai requisiti dell'AI Act. Tale documentazione deve contenere una descrizione completa del modello, incluse le politiche d'uso, la data di rilascio, le versioni del software, l'architettura e il numero di parametri, e i formati di input e output.

Un elemento chiave della documentazione è la descrizione dei dati di addestramento, comprendendo la loro provenienza, tipologia e organizzazione. Inoltre, le imprese devono spiegare le modalità con cui il modello interagisce con altri software o hardware. Gli obblighi di trasparenza si estendono anche alla natura dei contenuti addestrati, poiché è necessario indicare il rispetto del diritto d'autore nei dati utilizzati, un aspetto complesso poiché molti modelli utilizzano dati reperiti da internet senza una chiara distinzione sulla licenza o sulla proprietà intellettuale.

Questi requisiti di documentazione si applicano ai modelli commerciali e non riguardano i sistemi open source, dove l'architettura del modello, i pesi e le informazioni d'uso sono liberamente accessibili. Tuttavia, l'esenzione non si applica ai modelli generativi a rischio sistemico, poiché la natura del rischio elevato impone comunque il rispetto dei requisiti di trasparenza.

Obblighi aggiuntivi per modelli a rischio sistemico

L'articolo 55 impone ulteriori obblighi per i modelli generativi a rischio sistemico. I fornitori devono svolgere valutazioni di conformità che rispecchiano le migliori pratiche e devono analizzare i rischi associati al loro modello, avvisando immediatamente le autorità in caso di incidenti gravi.
Un incidente grave include decessi, gravi danni alla salute, violazioni di diritti fondamentali o impatti negativi su infrastrutture

critiche o l'ambiente. La registrazione e la segnalazione di tali eventi sono obbligatorie, con l'obiettivo di consentire alle autorità di vigilare sull'uso responsabile di questi modelli e di mitigarne gli effetti negativi.

Codici di buone pratiche e linee guida

L'articolo 56 introduce il concetto di "codici di buone pratiche," che fungeranno da linee guida per agevolare la conformità all'AI Act. La loro elaborazione è progettata per essere inclusiva e trasparente, coinvolgendo fornitori, sviluppatori e utenti di modelli IA generativi. Questo processo permetterà di raccogliere contributi da varie parti interessate e creare un set di buone pratiche condiviso. I codici di buona pratica dovrebbero essere pronti entro nove mesi dalla pubblicazione del regolamento e dovranno essere approvati dalla Commissione Europea. In futuro, questi codici saranno soggetti a revisioni periodiche per adattarsi ai cambiamenti tecnologici e all'esperienza pratica maturata.

Conclusioni

Il Capo V dell'AI Act è una risposta legislativa all'avvento dei modelli di intelligenza artificiale generativa, che hanno dimostrato capacità e rischi senza precedenti. L'AI Act non solo definisce le caratteristiche e i contesti applicativi di questi modelli, ma introduce una struttura normativa che obbliga le aziende a garantire trasparenza, sicurezza e rispetto delle norme di proprietà intellettuale. Inoltre, impone specifici obblighi per i modelli considerati a rischio sistemico, richiedendo alle aziende di documentare i dati di addestramento e di segnalare tempestivamente incidenti gravi. La classificazione dei modelli a rischio sistemico è basata su vari parametri, come la potenza di

calcolo utilizzata e la scala di utilizzo.

Gli articoli del Capo V mirano a regolamentare un settore in rapida evoluzione, introducendo misure concrete per ridurre i rischi e assicurare che i sistemi IA generativi operino in modo sicuro e conforme alle normative europee. La previsione dei codici di buone pratiche riflette un approccio inclusivo e flessibile, che consente alle aziende di adattarsi alle norme mentre la tecnologia e i contesti d'uso continuano a evolversi. In tal modo, l'AI Act cerca di bilanciare l'innovazione tecnologica con la tutela dei diritti fondamentali, della sicurezza e dell'integrità sociale, offrendo una base normativa che potrebbe servire come modello per future regolamentazioni globali.

Misure di sostegno

Il Capo VI dell'AI Act, con sette articoli, introduce misure di sostegno all'innovazione, ancora in fase di definizione e implementazione. Le principali sono gli "spazi di sperimentazione normativa per l'IA", ossia ambienti controllati dove fornitori e sviluppatori possono testare e validare sistemi di IA innovativi in condizioni reali, sotto la supervisione di autorità competenti e per un periodo limitato. Questi spazi offrono anche accesso preferenziale alle PMI e alle start-up, potenzialmente includendo l'uso dei supercomputer europei.

Oltre agli spazi sperimentali, la Commissione Europea, attraverso l'ufficio per l'IA, fornirà supporto all'innovazione creando modelli standardizzati per l'applicazione del Regolamento, una piattaforma informativa centralizzata, campagne di comunicazione e iniziative per armonizzare le pratiche di appalto pubblico relative ai sistemi di IA.

Queste misure mirano a facilitare la compliance delle imprese e a promuovere l'adozione sicura dell'IA in Europa.

Ultimi capi del regolamento (VII / XIII)

Gli ultimi capi dell'AI Act coprono una serie di aspetti chiave, tra cui governance, banca dati europea, monitoraggio, codici di condotta, sanzioni e disposizioni finali, fornendo un quadro completo per l'applicazione e il controllo della normativa sull'intelligenza artificiale.

Governance (Capo VII)

Il Capo VII delinea la governance, suddivisa tra livello dell'Unione Europea e nazionale. A livello europeo, l'Ufficio per l'IA, istituito dall'articolo 64, è l'organo principale per l'intelligenza artificiale, supportato dal Consiglio europeo per l'IA, composto da rappresentanti degli Stati membri e dal Garante europeo per la protezione dei dati come osservatore. Il Consiglio funge da intermediario tra Stati e Commissione, fornendo assistenza e consulenza per l'implementazione del Regolamento.

Il Forum consultivo, istituito dall'articolo 67, include rappresentanti dell'industria, start-up, PMI, società civile e mondo accademico, offrendo un equilibrio tra interessi economici e sociali. Il Gruppo di esperti scientifici, previsto dall'articolo 68, ha il compito di segnalare modelli di IA con rischio sistemico. A livello nazionale, ogni Stato deve istituire un'autorità di notifica e un'autorità di vigilanza del mercato (articolo 70) per garantire l'applicazione del Regolamento e gestire la conformità.

Banca dati dell'UE per i sistemi ad alto rischio (Capo VIII)

L'articolo 71 prevede la creazione di una banca dati europea per sistemi di IA ad alto rischio. Questa banca dati, gestita dall'Unione, raccoglierà informazioni dai fornitori e, in alcuni casi, dai deployer, per garantire una documentazione accurata e centralizzata. Questa misura mira a migliorare la tracciabilità e il controllo dei sistemi ad alto rischio.

Monitoraggio, vigilanza e condivisione delle informazioni (Capo IX)

Il Capo IX si occupa del monitoraggio successivo all'immissione sul mercato, in cui i fornitori e deployer devono vigilare sui loro sistemi, segnalando tempestivamente eventuali incidenti gravi alle autorità di vigilanza entro 15 giorni dall'identificazione. Sono stabilite procedure per la vigilanza e intervento sui sistemi la cui classificazione come ad alto o basso rischio è contestata. Il capitolo descrive le condizioni di "non conformità formale" e le misure da adottare per sistemi che non rispettano i requisiti.

Codici di condotta e orientamenti (Capo X)

L'articolo 95 del Capo X introduce codici di condotta volontari che promuovono l'applicazione dei requisiti previsti per i sistemi di IA ad alto rischio anche a sistemi a rischio inferiore. Questi codici, incoraggiati dall'Ufficio per l'IA e dagli Stati membri, sono destinati ai fornitori che scelgono volontariamente di adottare standard di gestione del rischio per garantire la trasparenza e sicurezza. Questa raccomandazione si estende anche ai deployer e serve a promuovere pratiche responsabili nell'uso dell'IA.

Delega di potere e procedura di comitato (Capo XI)

Il Capo XI conferisce alla Commissione il potere di adottare atti delegati, assistita da un comitato, per garantire l'adeguamento e l'aggiornamento delle disposizioni del Regolamento in base alle evoluzioni tecnologiche e alle esigenze di conformità.

Sanzioni (Capo XII)

Il Capo XII stabilisce sanzioni rigorose per chi viola il Regolamento, mirate a essere "efficaci, proporzionate e dissuasive". Le violazioni di sistemi IA che presentano rischi inaccettabili sono sanzionate fino a 35 milioni di euro o al 7% del fatturato globale dell'azienda, mentre le violazioni riguardanti sistemi ad alto rischio possono comportare multe fino a 15 milioni di euro o il 3% del fatturato. Anche i sistemi a rischio limitato sono soggetti a sanzioni per mancata trasparenza, con multe che arrivano fino a 15 milioni di euro o al 3% del fatturato. Le sanzioni variano a seconda della gravità delle infrazioni e saranno determinate dai singoli Stati membri in conformità alle linee guida del Regolamento.

Disposizioni finali (Capo XIII)

Il Capo XIII, articoli 102-113, contiene le disposizioni finali del Regolamento. Questo include l'elenco delle norme UE da aggiornare in conformità con l'AI Act, le modalità di gestione dei sistemi di IA già sul mercato, i processi di revisione della normativa e le date di entrata in vigore. Gli articoli 100 e 101 specificano le sanzioni per le istituzioni UE e i fornitori di modelli di IA per finalità generali.

Conclusioni

Questi ultimi capitoli dell'AI Act forniscono una struttura dettagliata per il monitoraggio e la governance dell'intelligenza artificiale in Europa. Tra le misure centrali vi sono la creazione di autorità di vigilanza a livello nazionale, una banca dati centralizzata per i sistemi ad alto rischio, sanzioni dissuasive per violazioni e un sistema di codici di condotta che incoraggia pratiche responsabili anche per sistemi non ad alto rischio. Il quadro complessivo mira a favorire la sicurezza e la trasparenza nell'uso dell'IA, promuovendo allo stesso tempo l'innovazione e l'adozione di standard condivisi.

Le agevolazioni per start up e PMI

Il Regolamento sull'Intelligenza Artificiale (AI Act) si propone di facilitare l'innovazione, prestando particolare attenzione alle necessità delle piccole e medie imprese (PMI) e delle start-up, che potrebbero incontrare ostacoli nella conformità normativa. Per questo motivo, il Regolamento include disposizioni per sostenere l'innovazione, tra cui l'articolo 62, che istituisce "spazi di sperimentazione normativa per l'IA" (regulatory sandboxes), ambienti controllati in cui le PMI possono sviluppare e testare sistemi di IA innovativi, anche ad alto rischio, in condizioni reali e sotto supervisione regolamentare.

L'articolo 62 richiede agli Stati membri di garantire alle PMI e alle start-up una via di accesso preferenziale a questi spazi, oltre a organizzare attività di sensibilizzazione e formazione specifiche. Inoltre, gli Stati devono offrire consulenze tecniche per facilitare la partecipazione delle PMI agli spazi di sperimentazione e promuovere il loro coinvolgimento nel processo normativo. Queste misure mirano a rendere più semplice e accessibile il percorso verso la conformità normativa, specialmente per le aziende emergenti.

Un altro aspetto rilevante riguarda le tariffe per la valutazione della conformità, che, secondo l'articolo 43, devono essere adattate alle necessità delle PMI, riducendo i costi in base alle dimensioni aziendali, mercato di riferimento o altri fattori. Anche nell'ambito dei codici di condotta (articolo 95), l'Ufficio per l'IA e gli Stati membri devono considerare le esigenze specifiche delle PMI, promuovendo la creazione di linee guida che permettano anche a sistemi non ad alto rischio di aderire volontariamente a standard di gestione del rischio.

Per quanto riguarda le sanzioni, l'articolo 99 prevede un regime agevolato per le PMI, suggerendo che le multe siano proporzionate alla loro capacità economica, anche se i dettagli sull'attuazione concreta di queste agevolazioni non sono ancora chiari. Infine, l'articolo 113 stabilisce che la revisione dell'AI Act, prevista entro il 2029 e successivamente ogni quattro anni, valuterà l'impatto della normativa sulle PMI, monitorando il numero di nuove imprese nel mercato dopo l'entrata in vigore del Regolamento.

In sintesi, il Regolamento prevede numerose agevolazioni e supporti per le PMI, tra cui accesso facilitato a spazi di sperimentazione e supercomputer dell'Unione, tariffe agevolate e sanzioni proporzionate, evidenziando l'intenzione di sostenere l'innovazione e la competitività delle imprese più piccole nel settore dell'IA.

"To do" delle imprese e monitoraggio

Questo capitolo offre alle imprese una guida per avviare da subito le attività di conformità necessarie ("To do") all'adeguamento all'AI Act. Nonostante molte scadenze e dettagli normativi debbano ancora essere chiariti, anticipare le azioni di conformità evita alle

aziende una corsa all'ultimo minuto e consente di sfruttare l'AI Act come strumento di innovazione, aiutandole a individuare e gestire meglio i progetti di IA.

Il percorso proposto prevede quattro azioni principali: **monitoraggio dei sistemi di IA presenti, analisi di tali sistemi, azioni correttive in base al monitoraggio e adeguamento dei processi aziendali**. La prima fase di monitoraggio implica un'analisi dettagliata dei sistemi e modelli di IA utilizzati dall'azienda. Anche se questo processo può sembrare semplice, nasconde alcune complessità, specialmente considerando la definizione di "sistema di IA" secondo il Regolamento, che include sistemi "automatizzati" con autonomia variabile e adattabilità post-diffusione, capaci di produrre output che influenzano ambienti fisici o virtuali.

Un'impresa, perciò, dovrebbe chiedersi se dispone di sistemi informatici con le caratteristiche definite dall'AI Act. Se un sistema è completamente statico e privo di adattabilità, non rientra nell'ambito dell'AI Act, anche se impiegato in settori ad alto rischio. Questa distinzione può aiutare a escludere alcune tecnologie non rilevanti e a concentrarsi sui sistemi di IA generativa che si stanno diffondendo rapidamente, come quelli incorporati nei tool di produttività. Questi sistemi non sono solo presenti su dispositivi aziendali, ma anche in cloud e applicazioni mobili, rendendo il monitoraggio complesso.

Il monitoraggio richiede la collaborazione dell'intera azienda e deve essere integrato con le procedure di cybersicurezza. Alcune domande utili per questa fase includono: *l'azienda distribuisce, sviluppa o utilizza sistemi di IA all'interno dell'Unione Europea? I suoi prodotti incorporano sistemi di IA? Rappresenta fornitori non stabiliti nell'UE che operano in questo mercato?* Queste

domande riguardano sia le aziende basate nell'UE sia quelle che, pur non essendo presenti nell'UE, distribuiscono prodotti nel suo.

Per creare un sistema di compliance efficace, il capitolo suggerisce di trasformare i requisiti normativi in una serie di domande strutturate, simili a un diagramma di flusso, dove ogni quesito guida il processo di verifica della conformità. Ad esempio, se un sistema di IA è identificato come pertinente, l'azienda dovrebbe chiedersi quali caratteristiche possiede, quali misure di controllo sono già state adottate e cosa manca per la conformità.

Un'analisi approfondita del Regolamento AI Act porta alla luce migliaia di queste domande di conformità, rendendo evidente la complessità e la profondità dell'adeguamento normativo. Pertanto, il capitolo fornisce solo una selezione di queste domande per aiutare le aziende a comprendere il processo e costruire una strategia di compliance solida. Con l'obiettivo di evitare rischi futuri e sfruttare il regolamento come catalizzatore di innovazione, le imprese dovrebbero dunque iniziare al più presto questo percorso di adeguamento.

Questo capitolo guida le aziende nel processo di classificazione dei sistemi di intelligenza artificiale (IA) per adempiere alle normative dell'AI Act. La classificazione inizia con un'analisi approfondita dei sistemi già monitorati, valutando il rischio intrinseco e il ruolo che ogni sistema ha nell'azienda. La procedura di classificazione dovrebbe essere condotta da personale competente sia in ambito informatico sia normativo, poiché richiede una comprensione dettagliata delle categorie normative dell'AI Act. La pubblicazione di linee guida e modelli standardizzati faciliterà il compito, ma un'analisi preliminare è necessaria per individuare tempestivamente le aree a rischio.

Esenzioni

Il primo passo è valutare se esistono cause di esenzione per alcuni sistemi di IA. Si devono considerare domande come: l'azienda utilizza l'IA esclusivamente per scopi militari, di difesa o sicurezza nazionale? Se i sistemi sono destinati solo a ricerca scientifica o scopi personali, potrebbero essere esentati dall'AI Act. Questa fase permette di escludere dall'analisi sistemi che non rientrano nel Regolamento.

Ruolo dell'azienda rispetto ai sistemi di IA

Successivamente, occorre determinare il ruolo dell'azienda in relazione a ciascun sistema o modello di IA, ovvero se agisce come **fornitore, deployer, distributore o importatore**. Ad esempio, un'azienda che sviluppa internamente un modello di IA e lo immette sul mercato con il proprio marchio è considerata fornitore. È utile creare un inventario dei sistemi di IA presenti, identificando per ciascuno il ruolo svolto dall'azienda. Le informazioni chiave da includere sono: il tipo di sistema, il reparto interessato, il ruolo dell'azienda e l'eventuale esenzione.

Classificazione del rischio

Una volta chiariti i ruoli e identificate le esenzioni, ogni sistema deve essere valutato per stabilire il livello di rischio intrinseco. Il primo aspetto è verificare se un sistema rientra tra quelli vietati dall'articolo 5 dell'AI Act – ciò include sistemi che utilizzano tecniche manipolative per influenzare il comportamento delle persone, quelli che sfruttano vulnerabilità legate a età, disabilità o condizioni socio-economiche e quelli che creano o ampliano banche dati di riconoscimento facciale attraverso scraping non autorizzato. Se un sistema rientra tra quelli vietati, l'azienda deve

cessare l'uso e informare tutti i soggetti coinvolti.

Per i sistemi di identificazione biometrica "in tempo reale" in spazi pubblici, è essenziale verificare che siano conformi alle normative locali e autorizzati da un'autorità indipendente. Inoltre, l'azienda deve tenere una documentazione dettagliata dell'uso e notificare alle autorità i casi di identificazione biometrica, in particolare quelli in cui vengono prese decisioni che hanno conseguenze legali significative.

Sistemi ad alto rischio e sistemi per finalità generali

I sistemi di IA ad alto rischio devono essere valutati secondo i criteri indicati negli allegati I e III del Regolamento. Questi includono settori come la sanità, il reclutamento, la giustizia e le infrastrutture critiche. Occorre chiedersi se il sistema in questione funge da componente di sicurezza, se è soggetto a valutazione da parte di terzi, e se il suo utilizzo comporta rischi significativi per la salute e i diritti fondamentali delle persone.

Inoltre, per i sistemi di IA generali e generali a rischio sistemico, è importante stabilire se presentano un impatto elevato o un rischio sistemico. Le soglie tecniche, come il numero di operazioni in virgola mobile per secondo (FLOPS) impiegate durante l'addestramento, aiutano a identificare tali rischi. La capacità di calcolo e il numero di utenti finali sono altri parametri che determinano se un sistema di IA presenta un rischio sistemico.

Obblighi di trasparenza

I sistemi che generano contenuti sintetici e deep fake o interagiscono direttamente con gli utenti sono soggetti agli

obblighi di trasparenza previsti dall'articolo 50. In questi casi, è obbligatorio informare gli utenti del coinvolgimento dell'IA nei contenuti o interazioni.

Etichettatura dei sistemi di IA

Dopo aver completato tutte le analisi, ogni sistema di IA in azienda deve essere catalogato in una delle seguenti categorie:

- Sistema vietato;
- Sistema ad alto rischio;
- Sistema di IA per finalità generale;
- Sistema di IA per finalità generale a rischio sistemico;
- Sistema soggetto a obblighi di trasparenza;
- Sistema non compreso nelle categorie precedenti.

Questa classificazione è essenziale per garantire la conformità normativa e per sviluppare strategie di gestione e monitoraggio personalizzate, assicurando che l'azienda sia pronta a rispondere ai requisiti dell'AI Act e a tutelare i propri interessi commerciali.

Le azioni sui programmi

Il capitolo descrive le azioni principali che le aziende devono intraprendere per conformarsi all'AI Act in base alla classificazione dei loro sistemi di intelligenza artificiale. Queste azioni riguardano tre categorie di sistemi: sistemi vietati, sistemi ad alto rischio e sistemi per finalità generali. Inoltre, sono previste azioni specifiche per garantire la trasparenza dei sistemi IA che interagiscono con persone o generano contenuti artificiali.

Sistemi vietati

Per i sistemi di IA vietati, la normativa richiede alle aziende di interrompere l'uso, la distribuzione e la vendita di questi sistemi entro il 2 febbraio 2025, salvo eccezioni specifiche previste dal regolamento. La cessazione di questi sistemi è essenziale per evitare sanzioni e rispettare i requisiti di sicurezza pubblica e tutela dei diritti fondamentali.

Sistemi ad alto rischio

Per i sistemi di IA classificati come ad alto rischio, le aziende devono implementare un rigoroso sistema di gestione dei rischi. Questo processo include l'elaborazione di una documentazione dettagliata della valutazione del rischio, che deve essere disponibile su richiesta delle autorità nazionali competenti. Le aziende devono dimostrare di aver adottato misure efficaci per prevenire o ridurre i rischi associati ai sistemi di IA e valutare periodicamente i rischi significativi per la salute, la sicurezza e i diritti fondamentali. Gli obblighi di conformità comprendono la verifica dello stato dell'arte della tecnologia e l'adozione di misure di attenuazione e controllo laddove i rischi non possano essere completamente eliminati.

Le aziende devono anche:

- Consultare le linee guida della Commissione per classificare correttamente i sistemi di IA ad alto rischio.
- Garantire che la documentazione tecnica e le procedure aziendali siano aggiornate e includano le informazioni necessarie ai deployer.
- Sottoporre i sistemi a prove rigorose per verificare che funzionino in modo conforme agli standard e siano idonei

all'uso previsto, tenendo conto dei potenziali impatti negativi su minori e persone vulnerabili.

- Presentare un piano di prova in condizioni reali all'autorità di vigilanza del mercato, assicurandosi che il sistema sia conforme ai requisiti della normativa di armonizzazione dell'Unione.

Oltre alle azioni tecniche e procedurali, è richiesto che l'azienda nomini **un rappresentante autorizzato** ubicato nell'Unione Europea. Questo rappresentante agisce per conto dell'azienda nei confronti delle autorità di regolamentazione, assicurando la conformità alle disposizioni del regolamento.

Sistemi di IA per finalità generali

Per i sistemi di IA per finalità generali, le aziende devono garantire che la documentazione tecnica del modello sia aggiornata e conforme ai requisiti previsti. La documentazione deve coprire l'intero processo di addestramento e prova, includendo elementi quali:

- Le funzioni del modello e il tipo di sistemi in cui può essere integrato.
- Politiche di utilizzo accettabili, architettura e parametri del modello, licenza e modalità di distribuzione.
- Specifiche di progettazione, informazioni sui dati di addestramento, prova e validazione, e risorse computazionali utilizzate per il modello.

Inoltre, le aziende devono fornire ai fornitori di sistemi di IA le informazioni tecniche necessarie affinché comprendano chiaramente le capacità e i limiti del modello, soprattutto per quanto riguarda l'eventuale integrazione del modello in altri sistemi di IA. Tra gli obblighi, l'azienda deve rispettare il diritto

d'autore, assicurandosi di non violare i diritti sui dati utilizzati durante l'addestramento. Prima di immettere un modello sul mercato, l'azienda deve nominare un rappresentante autorizzato nell'Unione, che gestirà i rapporti con le autorità di regolamentazione.

Le aziende che sviluppano modelli di IA a rischio sistemico devono inoltre valutare e mitigare i potenziali rischi per l'Unione Europea e adottare misure specifiche per ridurre i rischi a livello sistemico. È consigliato basarsi sui **codici di buone pratiche** per dimostrare la conformità agli obblighi normativi.

Azioni per la trasparenza

Per garantire la trasparenza, le aziende che utilizzano sistemi IA che interagiscono direttamente con le persone devono informare chiaramente gli utenti che stanno interagendo con un sistema di IA, a meno che non sia ovvio. Gli obblighi di trasparenza comprendono la marcatura di contenuti generati o manipolati artificialmente, come audio, video o testi, affinché siano facilmente riconoscibili come prodotti dall'intelligenza artificiale.

Per i sistemi di IA che eseguono **riconoscimento delle emozioni o identificazione biometrica**, l'azienda deve informare chiaramente le persone coinvolte sul funzionamento del sistema e assicurarsi che i dati personali siano trattati in conformità con il Regolamento Generale sulla Protezione dei Dati (GDPR). Se vengono creati contenuti "deep fake", è obbligatorio informare gli utenti dell'origine artificiale del contenuto, tranne quando l'uso è autorizzato a fini legali. Le informazioni devono essere fornite in modo chiaro e visibile durante la prima interazione.

Le aziende sono incoraggiate a partecipare all'elaborazione di

codici di buone pratiche per migliorare la conformità agli obblighi di trasparenza, collaborando con enti di regolamentazione e altre aziende del settore. Questi codici possono supportare l'azienda nel garantire che i contenuti generati dall'IA siano etichettati e riconoscibili in modo efficace.

Conclusione

In sintesi, le azioni previste dall'AI Act per le aziende che utilizzano o sviluppano sistemi di IA variano in base alla categoria di rischio del sistema. Per i sistemi vietati, l'azienda deve cessarne immediatamente l'uso e la distribuzione. I sistemi ad alto rischio richiedono l'implementazione di un sistema di gestione dei rischi e una documentazione dettagliata per garantire la conformità normativa e la sicurezza degli utenti. I modelli di IA per finalità generali devono essere documentati accuratamente e valutati per i potenziali rischi sistemici, con la nomina di un rappresentante autorizzato per i rapporti con le autorità. Infine, i sistemi IA soggetti agli obblighi di trasparenza devono informare chiaramente gli utenti, assicurando che i contenuti generati dall'IA siano etichettati in modo riconoscibile.

Questo quadro di azioni preventive e correttive supporta le aziende nel rispettare le disposizioni dell'AI Act, contribuendo allo sviluppo di un'intelligenza artificiale sicura e responsabile all'interno del mercato europeo.

Adeguamento dei processi

Il Regolamento sull'Intelligenza Artificiale impone alle aziende non solo di adattare singoli sistemi IA, ma anche di riorganizzare i propri processi aziendali complessivi per rispettare le nuove norme. Di seguito viene descritto un insieme di azioni fondamentali che le

aziende devono implementare per conformarsi, dal sistema di gestione del rischio alla documentazione e monitoraggio post-commercializzazione.

Sistema di gestione del rischio e qualità

Il regolamento richiede alle aziende un sistema di gestione del rischio che agisca su tutti i processi aziendali, similmente a un sistema di gestione della qualità. Questo sistema deve assicurare che i rischi derivanti dall'uso di IA siano identificati, valutati e gestiti. Alcuni aspetti da considerare includono:

- **Valutazioni d'impatto** sui diritti fondamentali nell'uso di IA, monitorando rischi elevati soprattutto in spazi di sperimentazione normativa.
- **Monitoraggio post-commercializzazione** per i sistemi ad alto rischio, che implica la raccolta e l'analisi continua dei dati sulle prestazioni per l'intero ciclo di vita del prodotto.
- **Cybersicurezza e protezione dei dati**: le aziende devono assicurare che i sistemi IA dispongano di misure per proteggere dati e informazioni sensibili, e che questi vengano eliminati una volta esaurito lo scopo per cui sono stati raccolti.

Gestione degli incidenti gravi

Il Regolamento richiede alle aziende di segnalare immediatamente qualsiasi incidente grave relativo ai sistemi IA ad alto rischio alle autorità di vigilanza. Per questo, devono essere predisposti processi per:

- **Segnalazione tempestiva** di incidenti, entro un massimo di 15 giorni in caso di nesso causale stabilito tra incidente e IA, e entro 10 giorni in caso di decesso.
- **Indagini e misure correttive** rapide in seguito a incidenti,

cooperando con le autorità.

- **La definizione di ruoli specifici** per chi si occupa di monitorare e intervenire in caso di incidenti, garantendo anche la protezione dei dati durante le operazioni.

Azioni per la commercializzazione

Le azioni necessarie per commercializzare sistemi di IA, in particolare quelli ad alto rischio, si dividono in azioni pre-commercializzazione e azioni post-commercializzazione.

Azioni pre-commercializzazione

Prima di mettere un sistema di IA sul mercato, le aziende devono:

- **Definire un sistema di gestione del rischio** che monitori i possibili impatti dei sistemi IA.
- **Creare un sistema di governance dei dati** per garantire l'integrità e l'uso appropriato dei dati.
- **Redigere la documentazione tecnica:** deve descrivere il funzionamento del sistema, il ciclo di vita, e includere informazioni dettagliate sui dati e le metodologie di addestramento.
- **Implementare un sistema di registrazione dei log** che permetta di tracciare eventi rilevanti per la sicurezza.
- **Assicurare la trasparenza** con strumenti informativi per gli utenti, assicurando la supervisione umana e il rispetto delle norme di cybersicurezza.

Inoltre, i sistemi IA ad alto rischio devono ottenere una **valutazione di conformità** e un certificato di conformità da un organismo notificato, basato su una verifica della qualità e della documentazione tecnica. È necessario anche redigere una **Dichiarazione di conformità UE** e registrare il sistema nella **Banca dati dell'UE** per i sistemi IA ad alto rischio.

Prima dell'immissione sul mercato, il sistema deve inoltre essere contrassegnato con la marcatura CE.

Azioni post-commercializzazione

Dopo l'immissione sul mercato, il regolamento impone alle aziende di attivare un **sistema di monitoraggio continuo** per i sistemi ad alto rischio, che documenti e analizzi i dati delle prestazioni, incluso il feedback dai deployer e altre fonti. Tale sistema garantisce la costante conformità dei sistemi IA ai requisiti del regolamento per tutta la durata del loro ciclo di vita.

Il monitoraggio deve essere accompagnato **da un sistema di comunicazione per gli incidenti gravi**. In caso di incidente, le aziende devono:

- Notificare tempestivamente l'incidente e le sue circostanze alle autorità.
- Avviare misure correttive e collaborare con le autorità di vigilanza.
- Rafforzare la sicurezza e l'efficacia dei sistemi attraverso miglioramenti basati sui risultati del monitoraggio e sugli incidenti riscontrati.

Trasparenza e informazioni per i deployer

Le aziende devono predisporre **informazioni complete** per i deployer, come istruzioni su come utilizzare i sistemi IA in sicurezza, i limiti del sistema e le sue capacità. Queste informazioni assicurano che i deployer siano consapevoli delle modalità d'uso, dei rischi e delle precauzioni necessarie, supportando l'utilizzo sicuro del sistema IA.

Documentazione e valutazione della conformità

Per i sistemi IA, la documentazione tecnica è fondamentale e deve essere disponibile per tutte le fasi del ciclo di vita del prodotto. Include informazioni dettagliate sul processo di sviluppo, i dati utilizzati per l'addestramento e il test, e una valutazione dei rischi. Inoltre, le aziende devono predisporre:

- **Misure di cybersicurezza** specifiche per l'infrastruttura fisica e digitale.
- **Prove tecniche** che dimostrino la conformità ai requisiti normativi.
- **Valutazioni periodiche** per garantire che i sistemi restino conformi alle norme e continuino a operare in sicurezza.

Compliance continua e consigli pratici

Le aziende sono incoraggiate a implementare queste misure in anticipo, anche prima delle scadenze ufficiali. La predisposizione di documentazione tecnica, sistemi di qualità e valutazione dei rischi può contribuire a evitare ritardi e sanzioni in fase di controllo. Prepararsi con largo anticipo è vantaggioso, considerando che molte disposizioni del regolamento saranno applicabili entro pochi mesi o anni.

In sintesi, l'AI Act richiede alle aziende di attivare un sistema di gestione complesso e integrato, che vada oltre la semplice messa a punto dei singoli sistemi IA, per coprire l'intera struttura e operatività aziendale. L'adeguamento ai requisiti del regolamento rappresenta una sfida, ma anche un'opportunità per innovare e migliorare la sicurezza e l'affidabilità dei sistemi IA, contribuendo a uno sviluppo sostenibile e responsabile dell'intelligenza artificiale.

Lo scadenziario dell'AI Act

Raccogliamo qui tutte le scadenze temporali che emergono dalla lettura del Regolamento.

Scadenza generale

2 agosto 2026: Applicazione definitiva dell'intero regolamento e creazione di tutti gli enti e organi previsti. (Art. 113).

Scadenze a carico delle imprese

Scadenza	Contenuto	Riferimenti
2 febbraio 2025	Disposizioni generali e pratiche vietate descritte ai Capi I e II	Art. 113
2 agosto 2025	Disposizioni sui modelli di IA per finalità generali come definiti al Capo V	Art. 113
2 agosto 2027	Gestione dei sistemi ad alto rischio sulla base dall'articolo 6, paragrafo 1	Art. 113
2 agosto 2027	Termine perché i modelli di IA per finalità generali immessi sul mercato prima del 2 agosto 2025 siano resi conformi al Regolamento.	Art. 111
2 agosto 2030	Termine per la messa a norma da parte di deployer e fornitori di sistemi ad alto rischio destinati a essere utilizzati dalle autorità pubbliche	Art. 111
31 dicembre 2030	Termine per la messa a norma dei "sistemi di IA che sono componenti di sistemi IT su larga scala istituiti dagli atti giuridici elencati nell'allegato X" (riferiti ad esempio al sistema di Schengen, visti, ingressi e uscite), purché messi in servizio prima del 2 agosto 2027	Art. 111

La tabella successiva riporta le scadenze a carico del sistema di governance. Si tratta di scadenze che hanno un impatto importante anche per le imprese perché, ad esempio, implicano la creazione degli enti cui si devono rivolgere le stesse imprese, la creazione dei punti di contatto, la pubblicazione dei codici di buone pratiche con i quali confrontarsi, nonché la revisione del Regolamento e la definizione di quelle linee guida indispensabili per la corretta applicazione del Regolamento stesso.

Scadenza	Contenuto	Riferimenti
2 agosto 2024 e poi ogni anno	La Commissione rivede gli elenchi delle pratiche vietate e dei sistemi ad alto rischio	Art. 112
2 agosto 2025	Messa in campo delle disposizioni sugli organismi notificati e sulla struttura di governance	Cons. 179 e Art. 113
2 agosto 2025	Definizione dei codici di buone pratiche	Cons. 179
2 agosto 2025	Applicabilità delle sanzioni da parte degli Stati membri (già notificate alla Commissione)	Cons. 179 e Art. 113
2 agosto 2025	Messa a disposizione del pubblico, da parte degli Stati membri, di un punto di contatto unico	Art. 70
2 agosto 2025	Relazione da parte degli Stati membri alla Commissione sullo stato delle risorse finanziarie e umane delle autorità nazionali competenti	Art. 70
2 agosto 2025	Messa in campo del sistema a tutela della riservatezza definito dall'articolo 78	Art. 113
2 agosto 2025	Definizione da parte della Commissione degli orientamenti per la comunicazione sugli incidenti gravi	Art. 73
2 agosto 2025	Messa in campo di tutto il sistema di governance descritto al Capo VII	Art. 113

2 agosto 2026	Orientamenti pratici da parte della Commissione per la definizione dei sistemi ad alto rischio, di quelli vietati, sulle norme della trasparenza	Art. 6
2 agosto 2026	Pubblicazione da parte della Commissione di un elenco esaustivo di esempi pratici di casi d'uso di sistemi di IA ad alto rischio e non ad alto rischio	Art. 6
2 agosto 2026	Istituzione di almeno un spazio di sperimentazione normativa per l'IA per Stato membro	Art. 57
2 agosto 2028 (e poi ogni quattro anni)	Relazione della Commissione al Parlamento Europeo sulle eventuali modifiche dell'elenco dei sistemi ad alto rischio, delle misure per la trasparenza, e del sistema di supervisione e di governance	Art. 112
2 agosto 2028	Valutazione da parte della Commissione del funzionamento dell'ufficio per l'IA e trasmissione della relazione al Parlamento europeo e al Consiglio	Art. 112
2 agosto 2028 (e poi ogni quattro anni)	Relazione della Commissione al Parlamento europeo e al Consiglio sullo sviluppo di prodotti della normazione relativi allo sviluppo efficiente sotto il profilo energetico di modelli di IA per finalità generali	Art. 112
2 agosto 2028 (e poi ogni tre anni)	Valutazione da parte della Commissione dell'impatto e dell'efficacia dei codici di condotta volontari	Art. 112
2 agosto 2029 (e poi ogni quattro anni)	La Commissione trasmette al Parlamento europeo e al Consiglio una relazione di valutazione e di riesame del Regolamento nel suo complesso ipotizzando anche l'eventuale creazione di un'agenzia apposita dell'Unione che ponga rimedio alle carenze individuate	Art. 112
2 agosto 2031	La Commissione effettua una valutazione dell'esecuzione del Regolamento e riferisce al Parlamento, al Consiglio e al Comitato economico e sociale, proponendo eventuali modifiche.	Art. 112

I punti da chiarire dell'AI Act e gli aggiornamenti

L'AI Act, nonostante sia giunto alla sua stesura definitiva, presenta ancora molti punti aperti, sia dal punto di vista concettuale che operativo. Diversi aspetti della legge, come alcune definizioni chiave e la creazione degli enti di governance, richiedono infatti chiarimenti e linee guida da parte della Commissione Europea e degli Stati Membri, necessarie per una corretta attuazione della normativa e per aiutare le aziende a conformarsi.

Punti critici da chiarire

Alcuni concetti del regolamento necessitano di precisazioni specifiche per evitare ambiguità. Tra questi rientra la definizione stessa di "sistema di IA" e la distinzione tra "deployer" (chi utilizza o integra un sistema IA) e "fornitore" (chi sviluppa o commercializza il sistema). Altri concetti rilevanti riguardano la distinzione tra modelli e sistemi di IA a finalità generale e la definizione dei parametri per determinare quando un modello IA presenta un impatto elevato o un rischio sistemico. L'articolo 96 incarica la Commissione di fornire orientamenti pratici su aspetti centrali come le procedure per i sistemi ad alto rischio, le pratiche vietate, le modalità per assolvere agli obblighi di trasparenza e la definizione di "modifica sostanziale" (necessaria per chiarire quando un deployer assume i ruoli di un fornitore). Inoltre, entro il 2 febbraio 2026, la Commissione dovrà pubblicare un elenco di casi pratici di uso di sistemi di IA ad alto e basso rischio, il quale contribuirà a chiarire meglio le applicazioni specifiche della normativa.

Enti di governance da istituire

Per rendere l'AI Act pienamente operativo, è prevista la creazione di diversi organismi di governance. Tra i principali figurano:

- L'Ufficio per l'IA, che coordinerà la gestione dell'AI Act a livello europeo.

- Il Consiglio europeo per l'IA, incaricato di assistere la Commissione e promuovere la cooperazione tra gli Stati Membri.
- Il Forum consultivo e il Gruppo di esperti scientifici indipendenti, che rappresentano un supporto tecnico e scientifico per la gestione della normativa.
- Le Autorità di notifica e vigilanza del mercato a livello nazionale, responsabili di supervisionare il rispetto della normativa.
- I punti di contatto unici, destinati a facilitare la comunicazione tra imprese e autorità nazionali, e la Banca dati dell'UE, che raccoglierà informazioni sui sistemi IA ad alto rischio.

Azioni operative richieste

Il Regolamento prevede anche una serie di azioni specifiche da attuare per supportare l'innovazione e guidare le aziende verso la conformità. Tra queste, la Commissione Europea è incaricata di:

1. Fornire modelli standardizzati per facilitare l'attuazione del regolamento.

2. Creare e mantenere una piattaforma informativa che renda disponibili risorse e informazioni rilevanti per gli operatori.

3. Organizzare campagne di sensibilizzazione e comunicazione per promuovere la conoscenza dell'AI Act.

4. Promuovere la convergenza delle migliori pratiche negli appalti pubblici relativi ai sistemi IA.

Ulteriori misure includono la definizione di codici di buone pratiche e codici di condotta. I codici di buone pratiche sono previsti soprattutto per i sistemi ad alto rischio e per garantire trasparenza nei sistemi IA che generano contenuti o interagiscono

con gli utenti. I codici di condotta, invece, introdotti dall'art. 95, saranno adottabili su base volontaria anche da fornitori e deployer di sistemi non sottoposti a obblighi di conformità, rappresentando una risorsa aggiuntiva per coloro che vogliono dimostrare un impegno proattivo verso l'etica e la sicurezza nell'uso dell'intelligenza artificiale.

In sintesi, la piena attuazione dell'AI Act richiede ancora numerosi passaggi e chiarimenti operativi, e richiederà alle aziende di adeguare i loro processi organizzativi e di governance. La Commissione e gli Stati Membri dovranno supportare questo processo attraverso enti di governance, linee guida e codici per agevolare la conformità e garantire una gestione responsabile dell'intelligenza artificiale.

APPROFONDIMENTO A CURA DI

Roberto Serra

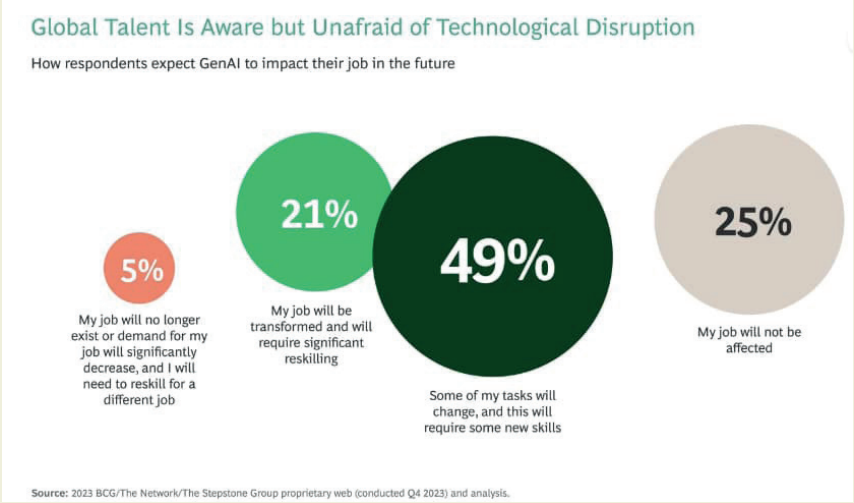
Esperto di marketing digitale
e Search Engine Optimization

IN ITALIA, L'INTELLIGENZA ARTIFICIALE NEL MONDO DEL LAVORO È ANCORA SOTTOVALUTATA

Nel nostro Paese l'intelligenza artificiale stenta a decollare: solo un lavoratore su cinque la utilizza e molti la sottovalutano, ignorando le opportunità che offre. Senza formazione e reskilling, il rischio è restare indietro mentre il resto del mondo corre.

Secondo un report del Boston Consulting Group, l'Italia è tra gli ultimi Paesi in Europa per adozione dell'IA. Il 40% non ha mai sperimentato questa tecnologia.

Solo un lavoratore italiano su cinque utilizza l'IA. Questo è quanto emerge da una ricerca del Boston Consulting Group (BCG). Quando ho letto questo dato, riportato anche da Il Sole 24 Ore, confesso che ho pensato si trattasse di un errore di battitura. Invece, approfondendo l'analisi, ho compreso come questo numero sia la spia di un problema molto più ampio, ovvero di una sottovalutazione diffusa di una tecnologia che sta rapidamente trasformando il mondo del lavoro. Pensa che secondo l'Implement Consulting Group, l'IA generativa potrebbe far crescere il PIL del Belpaese dell'8% in dieci anni (tra 150 e 170 miliardi di euro ogni anno)!



IA e mondo del lavoro italiano: storia di un amore non ancora sbocciato

La ricerca del BCG intitolata "Decoding Global Talent 2024", ha analizzato 150.000 lavoratori tra i 20 e i 40 anni in 188 paesi, Italia compresa, e i risultati sono sconcertanti.

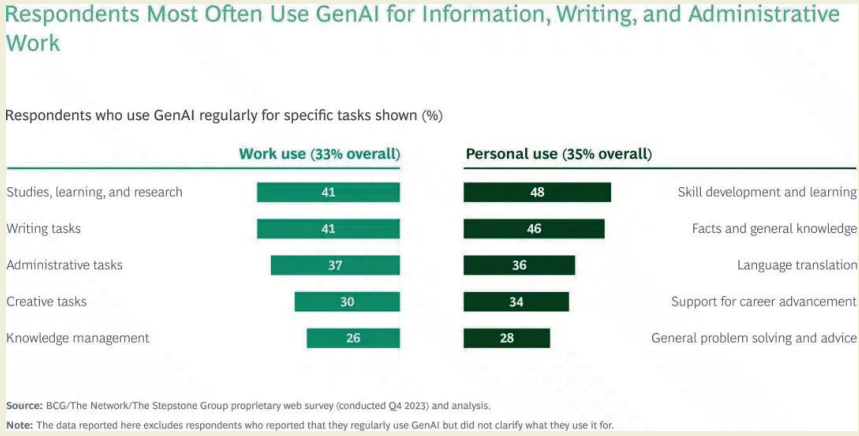
Sembra che i lavoratori italiani non siano particolarmente preoccupati dall'impatto dell'IA sul loro lavoro. Anzi, un buon 26% ritiene che l'IA non cambierà nulla, e solo un misero 7% ha paura di essere rimpiazzato. Il restante 49%? Beh, si aspetta qualche cambiamento, ma con un atteggiamento che sa tanto di "vedremo".

Sinceramente, a me viene un brivido a leggere questi dati. E a te?

Questa calma apparente è il frutto di una sottovalutazione colossale dell'intelligenza artificiale, come ci avverte Matteo Radice, Managing Director e Partner di BCG in Italia:

"Chi sottovaluta l'intelligenza artificiale rischia di perdere un'opportunità. Gli HR manager dovrebbero assumere un ruolo proattivo nell'informare e formare le persone, anche su competenze trasversali come problem solving e utilizzo di tecnologie innovative. L'IA può automatizzare alcune attività, specie le più ripetitive che non generano valore aggiunto e migliorarne altre".

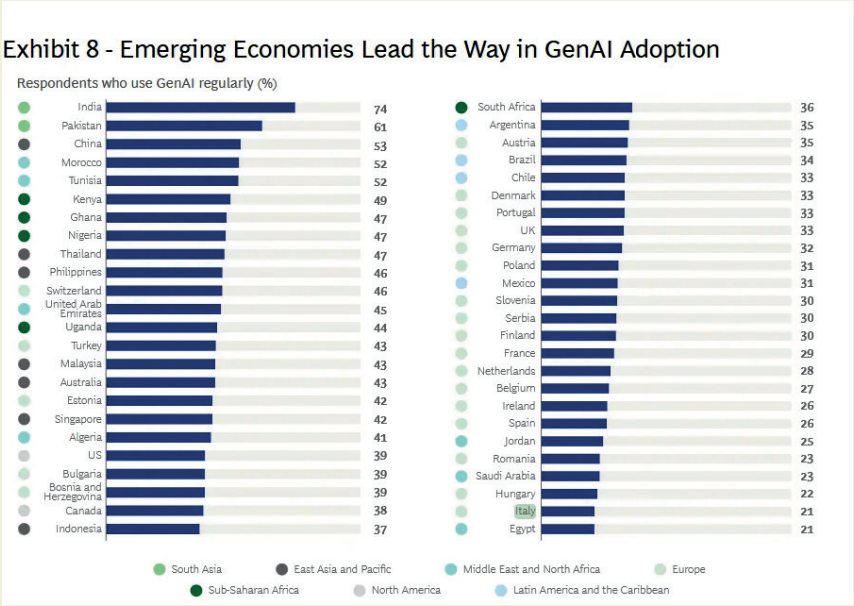
E prima lo capiamo, meglio è, aggiungo io. E tu, cosa ne pensi? Non credi che sia arrivato il momento di iniziare a prendere sul serio questa faccenda?



L'Italia, maglia nera d'Europa: uno spreco che non possiamo permetterci

Ma non finisce qui. Perché i dati peggiorano mano a mano che scendiamo nel dettaglio. Preparati a prendere appunti con la penna rossa: solo il 21% dei lavoratori italiani ha adottato in modo strutturato strumenti di IA nel proprio lavoro. Uno su cinque! Praticamente più di un terzo della forza lavoro italiana è ferma al palo, ignorando le infinite possibilità che questa tecnologia offre.

Nazioni come India e Pakistan, invece, stanno correndo a rotta di collo verso l'innovazione. Mentre noi? Ci troviamo a fare compagnia ai paesi del Medio Oriente nella classifica di chi usa meno l'IA. Un paradosso assurdo, non trovi?



Ma da cosa deriva questa disattenzione? Per me da una scarsa consapevolezza e informazione, oltre al fatto che il mondo del lavoro italiano non è giovane e rimane ancorato a pratiche del passato. Un fatto imperdonabile, specialmente se si vuole competere globalmente. Aggiungiamoci anche la miopia delle istituzioni che non incentivano le nuove tecnologie in azienda.

Insomma, un mix di pigrizia, disinformazione e un pizzico di presunzione, direi. Siamo un po' troppo convinti che la nostra routine quotidiana sia immune al cambiamento. Ma questa, come dovresti sapere, è una pia illusione.

Il reskilling: la tua arma segreta (se usata bene)

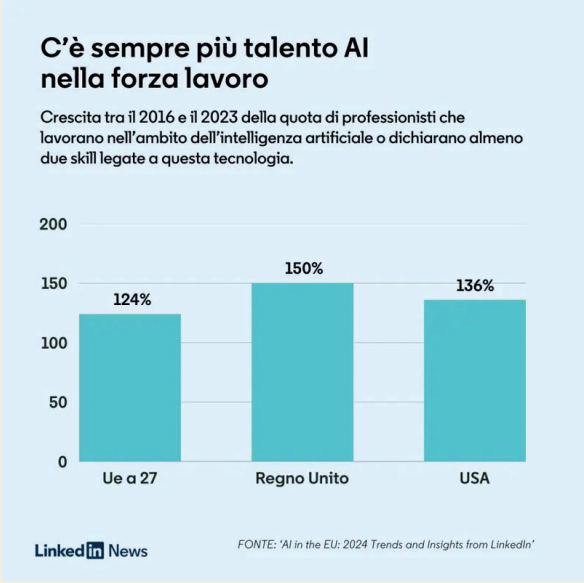
Non tutto è perduto, però. C'è una speranza, una piccola luce in fondo al tunnel: il 63% dei lavoratori italiani si dice disposto a intraprendere percorsi di reskilling per apprendere nuove competenze. Un dato incoraggiante, sulla carta, ma che deve tradursi in azioni concrete. Il reskilling non è una bacchetta magica. Serve un piano preciso, una strategia ben definita e, soprattutto, un cambio di mentalità.

Gli HR manager, in questo senso, devono essere lungimiranti, offrendo corsi di formazione mirati, sensibilizzando i dipendenti sul potenziale dell'IA e creando un ambiente di lavoro che favorisca l'innovazione.

Quindi, ti faccio una domanda diretta: cosa stai facendo tu, nella tua azienda, per preparare i tuoi collaboratori a questo cambiamento? Ti sei limitato a scaricare ChatGPT e a dire "fate voi"? Se la risposta è sì, perdona la brutalità, ti consiglio di cambiare registro.

LinkedIn suona la campana: l'IA è ormai una realtà in Europa

Se i dati di BCG non ti hanno convinto abbastanza, ecco un altro campanello d'allarme, questa volta da LinkedIn. Il suo report "AI in the EU: 2024 Trends and Insights" ha analizzato un miliardo di profili, e i risultati sono inequivocabili: in Europa, il numero di professionisti con competenze in IA è più che raddoppiato dal 2016, con una crescita del 124%. Un boom clamoroso.



Ma aspetta a esultare. Fuori da LinkedIn, siamo ancora una nicchia: solo lo 0,41% della forza lavoro europea ha competenze in IA. Il settore tecnologico è il primo attrattore, ma la crescita si fa sentire anche in finanza e nei servizi professionali, come si evince dal report di LinkedIn.

La domanda a questo punto è: la tua azienda è pronta a questo trend? Hai compreso che l'IA non è più un "nice to have", ma un "must have"? Se la risposta è no, forse è il momento di svegliarsi.

L'Asia corre mentre l'Occidente insegue a fatica

E non è finita qui. Perché, come spesso accade, il mondo non è un blocco monolitico, ma un mosaico di culture e percezioni diverse. E lo stesso vale per l'IA. Infatti, osservando i dati del 2024, emerge un divario abissale tra l'Occidente e l'Asia.

Da un lato, Stati Uniti, Regno Unito e Canada, dove lo scetticismo nei confronti dell'IA è palpabile. Un esempio? Negli USA il 45% della popolazione esprime preoccupazioni sugli effetti dell'IA!

In pratica, qui l'IA è vista come uno strumento utile, ma difficilmente capace di creatività e ragionamento avanzato. Un po' come se l'Occidente vedesse l'IA come un robot con le mani sporche di grasso, incapace di ragionamenti avanzati (niente di più sbagliato, come dovresti sapere!).

Dall'altra parte, in Paesi come Cina e Vietnam, c'è un entusiasmo che sfiora l'idolatria. Il 90% della popolazione vede l'IA come una grande opportunità, un motore di progresso economico e tecnologico. Qui, l'IA non è un nemico, ma un alleato, con il pieno supporto dei governi. Il nome Deep Seek, ti dice nulla?

Una differenza di percezione legata a fattori economici e sociali: in Occidente si ha paura che l'IA tolga il lavoro, mentre in Asia si spera che ne crei di più. Un paradosso che dovrebbe farti riflettere.

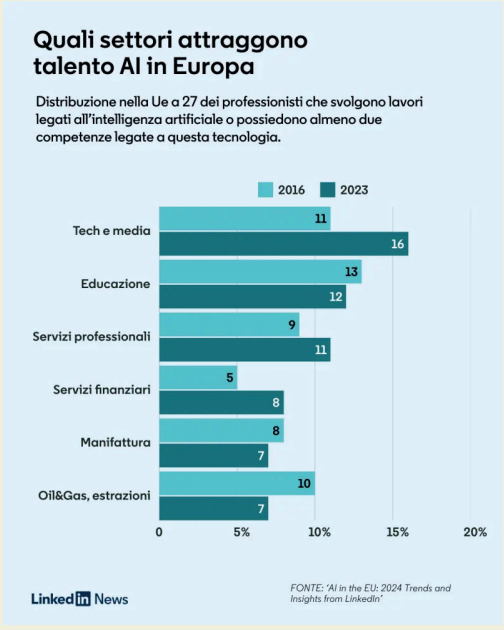
L'IA crea (e distrugge) lavoro

E arriviamo a un punto dirimente: l'IA crea nuove opportunità di lavoro? Ti riporto questi numeri, poi dimmi tu...

Il tasso di assunzione di talenti IA è aumentato del 78% rispetto al 2016. Un boom che ci dice che la domanda di esperti in IA è in

forte crescita. E dove crescono più velocemente le assunzioni? In Grecia (+263%), Portogallo (+193%) e Croazia (+178%), tre paesi che stanno puntando forte sull'innovazione, come puoi vedere tu stesso dal rapporto di LinkedIn.

Il settore tecnologico è ovviamente il principale datore di lavoro per i professionisti IA (16%), ma non solo: i servizi finanziari (8%), educazione (12%) e i servizi professionali (11%), sono seguiti da due settori molto "concreti" come il manifatturiero (7%) e l'oil & gas (7%).



Insomma, l'intelligenza artificiale, come uno tsunami, sta travolgendo ogni settore senza fare sconti. E non ti ho ancora parlato di impiegati virtuali...

Impiegati virtuali, automazione e gender gap: le realtà che non puoi ignorare

E adesso, una cosa molto concreta: l'arrivo degli impiegati virtuali. Sì, la tua azienda potrebbe essere affiancata da colleghi fatti di algoritmi e codici. Sempre più aziende, soprattutto startup e piccole imprese, stanno introducendo sistemi di IA capaci di gestire flussi di lavoro in completa autonomia.

Questi assistenti virtuali possono occuparsi di mansioni amministrative, assistenza clienti, analisi dati e gestione delle comunicazioni, consentendo alle aziende di crescere più velocemente e con costi ridotti.

Ma c'è anche un lato oscuro della medaglia: l'automazione. Il McKinsey Global Institute prevede che entro il 2030 il 30% delle ore lavorative negli Stati Uniti sarà automatizzato. Un dato che fa tremare i polsi. E i ruoli che si basano su compiti ripetitivi sono quelli più a rischio.

E attenzione, perché l'automazione non colpisce tutti allo stesso modo. Le donne, in particolare, sono risultate particolarmente vulnerabili all'impatto dell'IA, con una percentuale di posti di lavoro a rischio superiore rispetto agli uomini. Secondo un'analisi di Kenan Institute, l'80% delle posizioni lavorative ricoperte da donne è a rischio di automazione. Un dato inquietante che ci fa capire che la rivoluzione dell'IA rischia di accentuare le disuguaglianze di genere.

Solo il 26,3% dei professionisti AI in UE sono donne. E se le cose continuano così, ci vorranno 162 anni per raggiungere la parità di genere nel settore AI. Una situazione inaccettabile che dobbiamo

cercare di cambiare. Fortunatamente, alcuni paesi come Romania (33,9%), Finlandia (33,8%) e Francia (32,0%) stanno cercando di fare meglio.

Se l'Italia dorme, tu fatti trovare pronto!

E allora, cosa ne facciamo di tutti questi dati? Li ignoriamo, come sembra fare la maggior parte del nostro Paese, oppure decidiamo di affrontare la realtà a testa alta? L'Intelligenza Artificiale non è una minaccia aliena da cui fuggire, ma una forza concreta che potrebbe dare al mercato del lavoro italiano quella spinta che gli manca! Ignorarla, sottovalutarla, significa autoescludersi dalla partita, rimanere spettatori passivi di un cambiamento epocale.

Spero che questo approfondimento ti abbia fornito gli strumenti per comprendere la portata di questa trasformazione. Ti ho mostrato come, mentre il resto del mondo si prepara a cavalcare l'onda dell'IA, l'Italia sembra indugiare in un sonno profondo, pagando un prezzo altissimo in termini di opportunità perse e di crescita rallentata. Ma non è troppo tardi per invertire la rotta e affrontare il futuro con la preparazione adeguata.

Non lasciare che l'IA ti travolga come uno tsunami, ma impara a sfruttarne le potenzialità, a trasformarla in un'alleata per il tuo business. Non accontentarti di subire il cambiamento e reagire d'istinto, ma anticipalo e fatti trovare pronto.

APPROFONDIMENTO A CURA DI

Massimo Marini

Direttore commerciale di Analysis

CASE STUDY: USARE L'INTELLIGENZA ARTIFICIALE PER SEMPLIFICARE I PROCESSI DI GESTIONE DELLE INFORMAZIONI IN AZIENDA

Mi chiamo Massimo Marini e lavoro in Analysis, un'azienda che da 30 anni sviluppa software per rendere più efficienti i processi aziendali. Tra le soluzioni che offriamo, le più note sono Qualiware – una piattaforma che permette di gestire la compliance ai sistemi di Qualità, Sicurezza e Ambiente – e Activedoc, un software di gestione documentale che permette di integrare e centralizzare le informazioni aziendali in modo efficiente e strutturato.

L'intelligenza artificiale sta cambiando radicalmente il panorama della sicurezza aziendale e della gestione documentale. Ecco perché da qualche tempo abbiamo integrato l'IA nei nostri sistemi, in modo da poterne migliorare ulteriormente le performance. Questa integrazione consente infatti ai nostri clienti di automatizzare processi complessi, migliorare la precisione delle operazioni e ridurre il margine di errore umano.

Trasformare i processi aziendali con GPT

CoDriver, la nostra soluzione integrata con GPT, rappresenta il frutto di questa evoluzione. Essa si articola in diversi ambiti applicativi, ognuno dei quali sfrutta la potenza dell'intelligenza artificiale per trasformare processi tradizionali in attività automatizzate e "smart".

Estrazione dei dati da documenti (bollette, DDT, e-mail...)

Uno dei problemi più comuni nelle aziende è la gestione e la conservazione dei dati contenuti nei documenti e nelle e-mail. Grazie a *CoDriver*, siamo riusciti a sviluppare un sistema capace di estrarre e strutturare automaticamente le informazioni, rendendole immediatamente disponibili per l'integrazione con ERP e altri software gestionali. Un esempio concreto è l'estrapolazione di dati da bollette energetiche o DDT: il nostro sistema identifica e ricava i dati anche quando i documenti provengono da fonti diverse o coprono più stabilimenti. Nel caso dei DDT, ad esempio, una funzione di CoDriver consente di generare automaticamente un rapporto di accettazione partendo dal documento in formato PDF. Normalmente, in azienda, il data entry necessario per rendere leggibili i dati al gestionale richiede molte ore di lavoro. Grazie all'IA, questi dati possono essere estratti ed elaborati con estrema semplicità in pochi click.

Creazione del riesame della direzione

Uno dei compiti più strategici nella gestione aziendale è il riesame della direzione. Il nostro sistema è in grado di raccogliere e analizzare informazioni utili provenienti da audit, non conformità, reclami e segnalazioni, ed elaborare automaticamente una prima versione del riesame. In questo modo i responsabili hanno a disposizione un quadro chiaro delle criticità e delle opportunità

di miglioramento, che facilita la pianificazione strategica e l'eventuale adozione di misure correttive.

Risoluzione guasti intelligente

Un altro ambito in cui l'integrazione *CoDriver* si rivela estremamente utile è la manutenzione dei macchinari. Gli operatori possono formulare richieste in linguaggio naturale (anche a voce) e ricevere dal sistema risposte mirate, che si basano sulle informazioni presenti nel database e sullo storico delle manutenzioni. Oltre a suggerire soluzioni pratiche, CoDriver indica sempre anche le fonti consultate, garantendo trasparenza e affidabilità. Questa funzione risulta molto vantaggiosa quando si inserisce una nuova risorsa in azienda, ma anche quando gli operatori non parlano benissimo l'italiano o quando la documentazione dei macchinari è redatta in altre lingue, in quanto il sistema fa da intermediario e fornisce una traduzione automatica.

Tutti i vantaggi dell'implementazione

L'adozione di GPT nelle soluzioni QualiWare e ActiveDoc porta dunque con sé numerosi benefici:

- **Riduzione dei tempi di esecuzione** - Automatizzando le attività ripetitive, il lavoro degli operatori diventa più rapido ed efficiente.
- **Minimizzazione degli errori** - L'elaborazione automatizzata riduce il rischio di errori umani, aumentando l'affidabilità delle informazioni.
- **Supporto decisionale strategico** - Il riesame della direzione automatizzato fornisce una base solida per la pianificazione strategica, facilita la valutazione della performance e rende più semplice definire strategie di miglioramento.

- **Ottimizzazione della manutenzione** - La capacità di fornire risposte personalizzate alle richieste di risoluzione guasti garantisce interventi più tempestivi ed efficaci, contribuendo alla continuità operativa dell'azienda.

Alcune sfide legate all'implementazione

Ovviamente l'implementazione di soluzioni che usano l'IA nei processi aziendali presenta anche alcune difficoltà. Si tratta di aspetti di cui bisogna tener conto, in modo da riuscire ad aggirare gli ostacoli e ottenere il meglio dagli strumenti a disposizione.

- **Qualità dei dati**
  La qualità delle risposte fornite dall'intelligenza artificiale è direttamente proporzionale alla qualità dei dati messi a disposizione. Questo significa che, se la documentazione inserita è già curata e archiviata correttamente, le risposte saranno decisamente migliori.
- **Precisione delle risposte e validazione umana**
  Dobbiamo tenere in considerazione che l'IA attualmente non può garantire un'accuratezza totale. Il nostro sistema ha un range di risultati positivi dell'83-87%, una percentuale molto buona, ma naturalmente la verifica umana rimane assolutamente necessaria.
- **Formazione e coinvolgimento del team**
  Un'altro passaggio delicato è quello che riguarda il team, che deve essere convinto (e formato) ad usare questo nuovo strumento. Adottare una soluzione di questo tipo è un po' come passare da un'automobile tradizionale ad una con il cambio automatico: le prime due settimane si fa un po' fatica, perché bisogna abituarsi a ragionare in modo diverso. Ma una volta che si entra nel meccanismo e si capisce quanto è comodo, non si tornerebbe più indietro!

Noi di Analysis suggeriamo sempre di coinvolgere il personale già nel processo decisionale iniziale e nella prima fase di configurazione delle soluzioni, perché in questo modo le persone possono comprendere che l'IA non andrà a sostituire nessuno, ma che, al contrario, si tratta di un facilitatore in grado di portare giovamenti concreti e rendere più semplice il lavoro quotidiano.

Se vuoi saperne di più sulle nostre soluzioni, ti invito a visitare il nostro sito web: **www.qualiware.it**

Note sull'autore

Claudio Delaini

Mi sono appassionato alle regole sui prodotti durante l'Università. In verità io non amavo studiare Ingegneria, trovavo noioso fare tutti gli esercizi più e più volte. Andando in giro con papà ed entrando nelle fabbriche dei suoi clienti ho scoperto che i prodotti per essere venduti devono seguire delle regole, degli standard internazionali.

Ho scoperto i simboli, ho capito perché le etichette sono scritte in un certo modo... e mi sono innamorato! Io dico che è un po' come vedere il codice Matrix dietro ad ogni oggetto.

Il mio lavoro è nato così. Ho iniziato a raccontarlo prima con il blog, poi con YouTube e infine scrivendo libri. Tutto il resto è arrivato di conseguenza. Ah, un'ultima nota importante: ho seguito un master in Ingegneria Forense per saper difendere al meglio in tribunale i miei clienti in veste di consulente di parte.

Contributors

Roberto Serra

Roberto Serra è un esperto di SEO con approccio data driven. Nel corso degli anni si è specializzato nello sviluppo di progetti digitali all'avanguardia e nella consulenza SEO strategica per imprese di livello enterprise, con un focus particolare su metodologie innovative e non convenzionali. Tra le collaborazioni nel suo portfolio figurano aziende di rilievo come NGK Sparkplug, Fiera Milano, Fast Private Jet e altre.

È autore del saggio "Visibilità, il super potere che viene dal web", edito da Dario Flaccovio Editore, e ospite accreditato in numerosi eventi di settore e università. Viene considerato tra i SEO più innovativi del panorama nazionale per l'orientamento scientifico che ha dato alla materia.

Avvocato Silvia Zuanon

Laureata in Giurisprudenza a pieni voti all'Università degli Studi di Padova, svolge la pratica professionale presso lo studio B&P Avvocati di Verona, occupandosi prevalentemente di diritto ambientale, diritto amministrativo e diritto civile. Collabora quindi con varie aziende del nord Est fornendo consulenza in materia di contract management, gestione del rischio legale e diritto delle assicurazioni.

Conseguita l'abilitazione all'esercizio della professione, svolge un periodo di lavoro all'estero e successivamente, con l'Avv. Diana Michelazzo, fonda lo Studio MZ Avvocati all'interno del quale si occupa di diritto civile d'impresa e diritto societario nonché responsabilità amministrativa degli Enti dipendente da reato ex D.lgs. 231/2001 e Diritto Ambientale. Negli anni ha maturato una solida esperienza nella consulenza alle imprese, con particolare riferimento ai settori metallurgico, manifatturiero, agricolo e del terziario.

L'avv. Zuanon svolge altresì attività editoriale, di ricerca e formazione. Nel 2016 ha fondato e gestisce il blog Studiare Diritto Facile (www.studairedirttofacile.it) in materia di metodologia giuridica, unitamente al canale youtube Diritto Facile. Collabora inoltre con la società di formazione Insurance Lab pubblicando manuali in materia di diritto delle assicurazioni per la preparazione dell'esame IVASS. Ha pubblicato con la casa editrice CELT la Tribuna i manuali Diritto Penale Visivo e Diritto Civile Visivo.

Massimo Marini

Da oltre 15 anni si occupa di informatica, prima come tecnico poi come responsabile commerciale e infine come Direttore commerciale in Analysis. Grazie alle conoscenze acquisite negli anninegli di anni di studi edstudi e ed assistenza tecnica e alla capacità di relazionarsi, riesce a tradurre concetti informatici in maniera chiara e accessibile a chiunque.

Ad oggi ha aiutato più di 350 aziende nella digitalizzazione della compliance e dei processi.

Altre pubblicazioni

RSPP E VECCHI MACCHINARI IN FABBRICA

In molte aziende italiane, macchinari vecchi di decenni sono ancora in uso, spesso con documentazione incompleta o obsoleta.
Ma come possiamo assicurarci che questi strumenti siano conformi alle normative di sicurezza attuali?
Questo libro è una guida pratica per RSPP, datori di lavoro e professionisti della sicurezza che devono affrontare questa sfida quotidiana

di Claudio Delaini.

REGOLAMENTO MACCHINE 2023/1230

Questo libro è pensato per coloro che si trovano macchinari e attrezzature di lavoro costruite dal 1996 ad oggi. Quando capita un infortunio sul lavoro bisogna capire se la macchina industriale era conforme nell'anno di costruzione.

Ma anche quando bisogna marcare CE insiemi di macchine (con macchine nuove e macchine vecchie) bisogna aver chiaro come si sono evoluti i RES.

di Claudio Delaini e Stefano Boy

ROBOTICA E IMPRESA: COME AUTOMATIZZARE IL PRIMO IMPIANTO EVITANDO GLI ERRORI CHE FANNO TUTTI

Questo libro è pensato per chi sta pensando di comprare la sua prima isola robotica, ma anche per chi l'ha già fatto e ora si trova nei guai. Ti spieghiamo come progettare in modo intelligente, quali errori evitare, come affrontare le sicurezza e come rimediare se qualcosa è andato storto.

di Claudio Delaini e Fabio Bergamin

MARCATURA CE: CONCETTI BASE

Questo libro, vuole essere una guida introduttiva dedicata a tutti: sia ai fabbricanti con sede in Europa, sia agli importatori e distributori di prodotti provenienti dall'esterno dell'Unione Europea. Consideralo una specie di bignami per apprendere (o ripassare) i concetti fondamentali della marcatura CE.

di Claudio Delaini.

MANUALE DI USO E MANUTENZIONE DI UNA MACCHINA: COME REDIGERLO? COSA DEVE CONTENERE?

Il manuale d'uso delle macchine è un problema ricorrente nelle fabbriche: viene perso, è incompleto, non è in italiano, o, peggio, parla di macchine diverse da quella venduta!

Questo libro è utile a RSPP, consulenti sulla sicurezza e a chi deve scrivere o controllare il manuale

.di Claudio Delaini e Stefano Boy

FILTRI COL BOTTO

Usando un linguaggio semplice e moltissimi esempi pratici, ti spieghiamo quando le fabbriche sono a rischio esplosione, come funziona l'ATEX, come sono fatti gli impianti di depolverazione e come devono essere progettati per scongiurare i rischi e non trasformare il tuo capannone in una bomba ad orologeria.

di Claudio Delaini, Diego Perfettibile e Davide Pasini

IL CAOS DEI RECIPIENTI IN PRESSIONE

Questo libro è per i dirigenti, per gli RSPP, per i capo fabbrica e i preposti di stabilimento che hanno bisogno di districarsi facilmente e velocemente nelle normative sulla sicurezza dei macchinari e dei recipienti a pressione

di Claudio e Renato Delaini

NON DESIDERARE LA COLPA D'ALTRI. IL PRIMO COMANDAMENTO PER LA SICUREZZA DEI TUOI MACCHINARI

Analizziamo la Direttiva macchine e il Testo Unico 81, le leggi fondamentali per chiunque ha impianti industriali.

Leggerai suggerimenti e consigli nati sul campo in anni e anni d'esperienza e dritte su come applicare le norme che prese alla lettera sarebbero inapplicabili

di Claudio e Renato Delaini

LA DIRETTIVA ATEX SUI MACCHINARI. GUIDA PER CONSULENTI

Questo libro si concentra sulla Direttiva ATEX in relazione ai macchinari e delle attrezzature da lavoro.

È per i dirigenti di aziende manifatturiere, per gli RSPP, per i capo fabbrica e i preposti di stabilimento che hanno bisogno di districarsi facilmente e velocemente nelle normative sulla sicurezza dei macchinari.

di Claudio e Renato Delaini

IL MARCHIO CE È UN'ILLUSIONE. SECONDO COMANDAMENTO DELLA SICUREZZA DEI TUOI MACCHINARI.

Questo libro parla di quanto devi stare attento alla sicurezza dei tuoi macchinari. Non puoi fidarti solo del marchio CE, che è sostanzialmente un'autocertificazione! Con un sacco di esempi pratici, ti spieghiamo come prevenire e cosa fare in caso di guai.

di Claudio Delaini

INFORTUNIO SUL LAVORO? NON FARE LO STRUZZO! - TERZO COMANDAMENTO SULLA SICUREZZA DEI MACCHINARI

Se si infortuna una persona in fabbrica, come ci si deve comportare? Un libro per i direttori di stabilimento industriale, per i costruttori di macchine, per chi fa manutenzione industriale, ma anche per chi si occupa di diritto dei lavoratori e responsabilità di infortunio sul lavoro.

di Claudio e Renato Delaini

CERTIFICAZIONE CE PER CHI IMPORTA. INDICAZIONI ESSENZIALI PER GLI IMPORTATORI DA EXTRA UE

Un libro perfetto per tutti coloro che importano dalla Cina o comunque da extra EU. Le procedure e le regole valgono per aziende strutturate o importatori alle prime armi, ma spesso vengono ignorate finchè non arrivano i guai...

di Claudio e Renato Delaini

NON SCOTTARTI CON LA MOKA: GUIDA AI MOCA

Questa guida è stata scritta per i produttori di macchinari e di oggetti che sono destinati a venire a contatto con gli alimenti. Spieghiamo adempimenti e requisiti richiesti, nel modo più semplice possibile.

di Claudio e Renato Delaini

Fotografa il QR
per accedere a tutti i miei
riferimenti online